

## 国際調査報告

(法8条、法施行規則第40、41条)  
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 01/8036-SNY	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。	
国際出願番号 PCT/JP01/02992	国際出願日 (日.月.年) 06.04.01	優先日 (日.月.年) 06.04.00
出願人(氏名又は名称) ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。  
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

## 1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は

☐ 出願人が提出したものを承認する。

☒ 次に示すように国際調査機関が作成した。

携帯装置の記憶領域分割方法

5. 要約は

☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 1 図とする。☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F17/60, G06K17/00, G06K19/00, G09C1/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F17/60, G06K17/00, G06K19/00, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996  
 日本国公開実用新案公報 1971-2001  
 日本国実用新案登録公報 1996-2001  
 日本国登録実用新案公報 1994-2001

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 11-120300 A (富士通株式会社) 30.4月.1999 (30.04.99) 全文, 全図 & EP 908855 A2 & US 6003113 A1 & CN 1214488 A	1-30

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」 口頭による開示、使用、展示等に言及する文献  
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」 同一パテントファミリー文献

国際調査を完了した日

18.07.01

国際調査報告の発送日

31.07.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
 郵便番号100-8915  
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

前田 仁

5N

2945

電話番号 03-3581-1101 内線 6915

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P 1 0 - 1 0 5 4 7 2 A (株式会社東芝) 2 4 . 4 月 . 1 9 9 8 ( 2 4 . 0 4 . 9 8 ) 全文, 全図 & E P 7 9 8 6 7 4 A 2 & U S 5 9 2 9 4 2 8 A 1 & C N 1 1 7 4 3 5 5 A	1 - 3 0
A	J P 9 - 1 2 8 5 0 5 A (凸版印刷株式会社) 1 6 . 5 月 . 1 9 9 7 ( 1 6 . 0 5 . 9 7 ) 全文, 全図 (ファミリーなし)	1 - 3 0

# 明 細 書

## 携帯装置の記憶領域分割方法

### 技術分野

本発明は、複数のサービス提供元のサービスを単体のＩＣ(Integrated Circuit)カードを用いて提供可能にするデータ処理方法およびそのシステム、携帯装置、データ処理装置およびその方法とプログラムに関する。

### 背景技術

従来、ＩＣカードシステムにおいては、個人が携帯するＩＣカードに各種個人の情報等を記録し、駅の改札、部屋の入退出の管理等に使用するようになされている。

これに対して同種のカード形状の媒体として、例えばプリペイカード、各店舗が発行するサービス用のカード、各ソフトメーカーが発行するユーザーカード等が利用されるようになされている。

これらのカードにおいては、ＩＣカードを含めて、それぞれ各カードに係るサービス提供元(事業者)が個別に発行して利用に供されるようになされている。

ところでＩＣカードにおいては、内蔵のメモリに複数のサービスに係る情報を十分に記録可能な容量を確保することができることにより、複数の事業者でＩＣカードを共同使用することができると考えられる。

このようにすればそれまでカードを発行していた事業者においては、カード発行の負担を軽減することができ、また個々の事業者では獲得困難な多数のユーザーを獲得することもできる。またユーザーにおいては、携帯して管理するカードの枚数を少なくすることができることにより、多数のカードを携帯、管理する煩

雑さから開放されることになる。

ところがこのようにＩＣカードを複数の事業者で共同使用する場合、１人の事業者が専用のＩＣカードを発行する場合に比して、種々の要求に対応することが必要になる。すなわち事業者によっては、他の事業者とＩＣカードを共同使用する場合でも、あたかも自らが発行したＩＣカードのような使い勝手を望む場合も考えられる。また特定の事業者との間では、ＩＣカードの共同使用を望まない場合も考えられる。また共同使用する側で負担の軽減が要求される場合も考えられる。

本発明は以上の点を考慮してなされたもので、複数の事業者で単体のＩＣカード等を共用使用する場合に、サービス提供元のセキュリティの面を含む各種要望に対応することができるデータ処理方法およびそのシステム、携帯装置、データ処理装置およびその方法とプログラムを提供することを目的とする。

### 発明の開示

上述した目的を達成するために、第１の発明のデータ処理方法は、分割用鍵データおよび第１の領域管理鍵データを記憶する集積回路であって、前記第１の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される集積回路を搭載した携帯装置が、前記記憶領域を用いてサービスを提供する第１のサービス提供元によって発行された場合に、第２のサービス提供元に前記集積回路の前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理方法であって、前記分割用鍵データを管理する記憶領域運用元が、第２の領域管理鍵データを含む第１のモジュールデータを前記分割用鍵データで暗号化して前記第１のサービス提供元に提供し、前記携帯装置の発行元である前記第１のサービス提供元が、前記暗号化された第１のモジュールを含む第２のモジュールデータを前記第１の領域管理鍵データを用いて暗号化して前記記憶領域運用元

に提供し、前記記憶領域運用元の管理下で、前記暗号化された第2のモジュールデータを前記集積回路に提供し、前記集積回路内で前記第1の領域管理鍵データを用いて前記第2のモジュールデータを復号し、当該復号された第2のモジュール内の前記第1のモジュールデータを前記分割鍵データを用いて復号し、当該復号によって得られた前記第2の領域管理鍵データを用いて、前記記憶領域を前記第1のサービス提供元のサービスに用いられる第1の記憶領域と前記第2のサービス提供元のサービスに用いられる第2の記憶領域とに分割する。

上述した第1のデータ処理方法では、集積回路内で第2のモジュールが復号され、集積回路が第2の領域管理鍵データを得ることを条件に、第2のサービス提供元のサービスに用いられる第2の記憶領域が適切に形成される。

このとき、第1のモジュールは、分割用鍵データで暗号化されているため、当該第2のモジュールに含まれる第2の領域管理鍵データの内容は、第1のサービス提供元に秘密にできる。そのため、第1のサービス提供元は、記憶領域運用元に無断で第2のモジュールを不正に生成できない。

また、第2のモジュールは、第1の領域管理鍵データで暗号化されており、当該第1の領域管理鍵データは、第2のサービス提供元には秘密にされる。そのため、記憶領域運用元は、第1のサービス提供元に無断で第2のモジュールを不正に生成できない。

すなわち、第1の領域管理鍵データおよび分割用鍵データの双方を用いなければ第2のモジュールを生成できないため、第2の記憶領域の生成時に必要な第2の領域管理鍵データを集積回路が得られない。

また、第2のサービス提供元には、分割用鍵データおよび第1の領域管理鍵データの双方を秘密にしているため、第2のサービス提供元は第2のモジュールを生成できない。

これにより、第1のサービス提供元、記憶領域運用元および第2のサービス提供元が適切に連携して処理を行わないかぎり、集積回路内には第2の記憶領域が

形成されないため、高いセキュリティが実現できる。

また、第1の発明のデータ処理方法は、好ましくは、前記集積回路は、前記第1の領域管理鍵データを用いることを条件にデータの書き込みおよびデータの書き換えの少なくとも一方が許可される前記第1の記憶領域と、前記第2の領域管理鍵データを用いることを条件にデータの書き込みおよびデータの書き換えの少なくとも一方が許可される前記第2の記憶領域とに、前記記憶領域を分割する。

また、第1の発明のデータ処理方法は、好ましくは、前記集積回路は、第1のシステム鍵データをさらに記憶し、前記第1のシステム鍵データおよび前記第1の領域管理鍵データを用いることを条件に、前記記憶領域へのデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可し、前記記憶領域運用元は、第2のシステム鍵データをさらに含む第1のモジュールデータを前記分割用鍵データで暗号化して第1のサービス提供元に提供し、前記第1のサービス提供元は、前記暗号化された第1のモジュールと、前記記憶領域を他のサービス提供元に分割して利用させる条件を示す分割条件情報とを含む第2のモジュールデータを前記第1の領域管理鍵データを用いて暗号化して前記記憶領域運用元に提供し、前記集積回路内で前記第1の領域管理鍵データを用いて前記第2のモジュールデータを復号し、当該復号された第2のモジュール内の前記第1のモジュールデータを前記分割鍵データを用いて復号し、当該復号によって得られた前記第2のシステム鍵データ、第2の領域管理鍵データおよび前記分割条件情報を用いて、前記記憶領域の分割を行う。

また、第2の発明のデータ処理システムは、分割用鍵データおよび第1の領域管理鍵データを記憶する集積回路であって、前記第1の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される集積回路を搭載した携帯装置が、前記記憶領域を用いてサービスを提供する第1のサービス提供

元によって発行された場合に、第2のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理システムであって、前記分割用鍵データを管理する記憶領域運用元が使用する記憶領域運用処理装置と、前記携帯装置の発行元である前記第1のサービス提供元が使用する第1のサービス提供元処理装置と、前記第1のサービス提供元が使用する第2のサービス提供元処理装置とを有し、前記記憶領域運用処理装置は、第2の領域管理鍵データを含む第1のモジュールデータを前記分割用鍵データで暗号化して前記第1のサービス提供元処理装置に送信し、前記第1のサービス提供元処理装置は、受信した前記暗号化された第1のモジュールを含む第2のモジュールデータを前記第1の領域管理鍵データを用いて暗号化して前記記憶領域運用処理装置に送信し、前記記憶領域運用処理装置は、受信した前記暗号化された第2のモジュールデータを前記集積回路に提供し、前記集積回路は、前記第1の領域管理鍵データを用いて前記第2のモジュールデータを復号し、当該復号された第2のモジュール内の前記第1のモジュールデータを前記分割用鍵データを用いて復号し、当該復号によって得られた前記第2の領域管理鍵データを用いて、前記記憶領域を前記第1のサービス提供元のサービスに用いられる第1の記憶領域と前記第2のサービス提供元のサービスに用いられる第2の記憶領域とに分割する。

また、第3の発明の携帯装置は、第1のサービス提供元がサービスを提供するために用いられる集積回路を搭載した携帯装置であって、前記集積回路は、第2のサービス提供元に当該集積回路の記憶領域の一部を用いたサービスを提供させる処理を行う記憶領域運用元によって管理される分割用鍵データと、第1の領域管理鍵データとを記憶する記憶手段と、前記記憶領域運用元が発行した第2の領域管理鍵データを含むモジュールであって、前記記憶領域運用元が前記分割用鍵データを用いて暗号化し、さらに前記第1のサービス提供元が前記第1の領域管理鍵データを用いて暗号化したモジュールを入力する入力手段と、前記分割用鍵データおよび前記第1の領域管理鍵データを用いて、前記入力されたモジュール



を復号し、当該復号された前記モジュール内の前記第 2 の領域管理鍵データを用いて、前記記憶手段の記憶領域を第 1 の記憶領域と第 2 の記憶領域とに分割し、前記第 1 の領域管理鍵データを用いることを条件に前記第 1 の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可し、前記第 2 の領域管理鍵データを用いることを条件に前記第 2 の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可する処理手段とを有する。

また、第 4 の発明のデータ処理装置は、分割用鍵データ、第 1 のサービス提供元を識別するためのシステムコードおよび第 1 の領域管理鍵データを記憶する集積回路であって、前記第 1 の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可される集積回路を搭載した携帯装置が、前記記憶領域を用いて第 1 のサービスを提供する第 1 のサービス提供元によって発行された場合に、第 2 のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理装置であって、記憶手段と、処理手段と、入出力手段とを有し、前記記憶手段は、前記第 1 のサービス提供元および前記第 2 のサービス提供元によって提示された、同じ前記集積回路でサービスを提供可能なサービス提供元を特定するための拒絶情報を記憶し、前記処理手段は、第 2 の領域管理鍵データを含む第 1 のモジュールを前記分割用鍵データを用いて暗号化し、前記入出力手段は、前記暗号化された第 1 のモジュールを前記第 1 のサービス提供元に提供するために出力し、前記暗号化された第 1 のモジュールを含み前記第 1 のサービス提供元において前記第 1 の領域管理鍵データを用いて暗号化された第 2 のモジュールを入力し、前記第 2 のモジュールを、前記集積回路の記憶領域の一部を第 2 のサービス提供元が利用可能となるように前記第 2 のサービス提供元の管理下で前記記憶領域を分割する記憶領域分割装置に提供するために出力し、前記処理手段は、前記拒絶情報に基づいて、前記第 2 のサービス提供元と同じ前記集積回路で

サービスを提供可能な前記第 1 のサービス提供元に付与された前記システムコードを示す登録可能システムコードリストを生成し、前記入出力手段は、前記記憶領域分割装置に提供するために前記システムコードリストを出力する。

また、第 5 の発明のデータ処理装置は、分割用鍵データ、第 1 のサービス提供元を識別するためのシステムコードおよび第 1 の領域管理鍵データを記憶する集積回路であって、前記第 1 の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可される集積回路を搭載した携帯装置が、前記記憶領域を用いて第 1 のサービスを提供する第 1 のサービス提供元によって発行された場合に、第 2 のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理装置であって、記憶手段と、入出力手段と、処理手段とを有し、前記記憶手段は、当該データ処理装置の処理を管理する記憶領域運用元が発行した第 2 の領域管理鍵データを含むモジュールであって、前記記憶領域運用元が前記分割用鍵データを用いて暗号化し、さらに前記第 1 のサービス提供元が前記第 1 の領域管理鍵データを用いて暗号化したモジュールと、前記第 2 のサービス提供元と同じ前記集積回路でサービスを提供可能な前記第 1 のサービス提供元に付与された前記システムコードを示した登録可能システムコードリストとを記憶し、前記入出力手段は、前記集積回路から前記システムコードを入力し、前記処理手段は、前記入力したシステムコードが、登録可能システムコードリストに示されたものであると判断した場合に、前記入出力手段を介して前記モジュールを前記集積回路に出力する。

また、第 6 の発明データ処理装置は、第 1 の領域管理鍵データを用いることを条件に第 1 のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第 1 の記憶領域と、第 2 の領域管理鍵データを用いることを条件に第 2 のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第 2 の記憶領域とを有するに

集積回路の前記第 2 の記憶領域に前記ファイルデータを書き込む処理を行うデータ処理装置であって、前記第 2 の記憶領域内に複数の第 3 の記憶領域が規定され、前記複数の第 3 の記憶領域の各々について当該第 3 の記憶領域へのデータの書き込みおよび当該第 3 の記憶領域内のデータの書き換えの少なくとも一方を行うために用いられる第 3 の領域管理鍵データが規定されており、前記集積回路が前記第 3 の領域管理鍵データを記憶している場合に、前記第 3 の領域管理鍵データと、前記第 2 のサービスの提供者によって発行され、前記第 3 の記憶領域に前記ファイルデータを書き込む際に用いられ、前記第 3 の領域管理鍵データで暗号化されたファイル鍵データとを記憶する記憶手段と、前記暗号化されたファイル鍵データを前記集積回路に出力する出力手段と、前記ファイル鍵データを用いて、前記集積回路の前記第 2 の記憶領域に、前記第 2 のサービスの提供に用いられるファイルデータを書き込む書き込み手段とを有する。

また、第 7 の発明の携帯物発行方法は、分割用鍵データおよび第 1 の領域管理鍵データを記憶し、前記第 1 の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される集積回路を搭載した携帯物を発行し、前記分割用鍵データを用いて、前記第 1 の領域管理鍵データを用いることを条件にデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される第 1 の記憶領域と、第 2 の領域管理鍵データを用いることを条件にデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される第 2 の記憶領域とに前記集積回路の前記記憶領域を分割することを、前記分割用鍵データを管理する記憶領域運用元に依頼する。

また、第 8 の発明のプログラムは、分割用鍵データ、第 1 のサービス提供元を識別するためのシステムコードおよび第 1 の領域管理鍵データを記憶する集積回路であって、前記第 1 の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも

も一方を許可される集積回路を搭載した携帯装置が、前記記憶領域を用いて第1のサービスを提供する第1のサービス提供元によって発行された場合に、第2のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理をコンピュータに実行させるプログラムであって、前記集積回路から前記システムコードを入力する手順と、前記第2のサービス提供元と同じ前記集積回路でサービスを提供可能な前記第1のサービス提供元に付与された前記システムコードを示した登録可能システムコードリストを参照し、前記入力したシステムコードが、前記登録可能システムコードリストに示されたものであるか否かを判断する手順と、前記入力したシステムコードが、登録可能システムコードリストに示されたものであると判断した場合に、当該プログラムの実行を管理する記憶領域運用元が発行した第2の領域管理鍵データを含むモジュールであって、前記記憶領域運用元が前記分割用鍵データを用いて暗号化し、さらに前記第1のサービス提供元が前記第1の領域管理鍵データを用いて暗号化したモジュールを前記集積回路に出力する手順とを前記コンピュータに実行させる。

また、第9の発明のデータ処理方法は、分割用鍵データ、第1のサービス提供元を識別するためのシステムコードおよび第1の領域管理鍵データを記憶する集積回路であって、前記第1の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可される集積回路を搭載した携帯装置が、前記記憶領域を用いて第1のサービスを提供する第1のサービス提供元によって発行された場合に、第2のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理方法であって、前記集積回路から前記システムコードを入力する手順と、前記第2のサービス提供元と同じ前記集積回路でサービスを提供可能な前記第1のサービス提供元に付与された前記システムコードを示した登録可能システムコードリストを参照し、前記入力したシステムコードが、前記登録可能システムコードリストに示されたものであるか否かを判断する手順と、前記入力し

たシステムコードが、前記登録可能システムコードリストに示されたものであると判断した場合に、当該プログラムの実行を管理する記憶領域運用元が発行した第２の領域管理鍵データを含むモジュールであって、前記記憶領域運用元が前記分割用鍵データを用いて暗号化し、さらに前記第１のサービス提供元が前記第１の領域管理鍵データを用いて暗号化したモジュールを前記集積回路に出力する手順とを有する。

また、第１０の発明のプログラムは、第１の領域管理鍵データを用いることを条件に第１のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第１の記憶領域と、第２の領域管理鍵データを用いることを条件に第２のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第２の記憶領域とを有するに集積回路の前記第２の記憶領域に前記ファイルデータを書き込む処理をコンピュータに実行させるプログラムであって、前記第２の記憶領域内に複数の第３の記憶領域が規定され、前記複数の第３の記憶領域の各々について当該第３の記憶領域へのデータの書き込みおよび当該第３の記憶領域内のデータの書き換えの少なくとも一方を行うために用いられる第３の領域管理鍵データが規定されており、前記集積回路が前記第３の領域管理鍵データを記憶している場合に、前記第２のサービスの提供者によって発行され、前記第３の記憶領域に前記ファイルデータを書き込む際に用いられ、前記第３の領域管理鍵データで暗号化されたファイル鍵データを、前記集積回路に出力する手順と、前記ファイル鍵データを用いて、前記集積回路の前記第２の記憶領域に、前記第２のサービスの提供に用いられるファイルデータを書き込む手順とを前記コンピュータに実行させる。

また、第１１の発明データ処理方法は、第１の領域管理鍵データを用いることを条件に第１のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第１の記憶領域と、第２の領域管理鍵データを用いることを条件に第２のサービスの提供に用いられるファイルデータの書

き込みおよび書き換えの少なくとも一方が許可される第２の記憶領域とを有するに集積回路の前記第２の記憶領域に前記ファイルデータを書き込む処理を行うデータ処理方法であって、前記第２の記憶領域内に複数の第３の記憶領域が規定され、前記複数の第３の記憶領域の各々について当該第３の記憶領域へのデータの書き込みおよび当該第３の記憶領域内のデータの書き換えの少なくとも一方を行うために用いられる第３の領域管理鍵データが規定されており、前記集積回路が前記第３の領域管理鍵データを記憶している場合に、前記第２のサービスの提供者によって発行され、前記第３の記憶領域に前記ファイルデータを書き込む際に用いられ、前記第３の領域管理鍵データで暗号化されたファイル鍵データを、前記集積回路に出力する手順と、前記ファイル鍵データを用いて、前記集積回路の前記第２の記憶領域に、前記第２のサービスの提供に用いられるファイルデータを書き込む手順とを有する。

#### 図面の簡単な説明

図１は、本発明の実施形態に係わる通信システムの全体構成図であり、

図２は、図１に示すＩＣカードの機能ブロック図であり、

図３は、ＩＣカード発行者による発行後、カード記憶領域運用者による運用処理前に、図２に示すＩＣカードの記憶部に記憶されているデータを説明するための図であり、

図４は、図１に示す発行者用通信装置１１の機能ブロック図であり、

図５は、図１に示す運用者用通信装置１２の機能ブロック図であり、

図６は、図１に示す記憶領域分割装置の機能ブロック図である。

図７は、図１に示す運用ファイル登録装置の機能ブロック図であり、

図８は、図１に示す通信システムの全体動作の概要を説明するためのフローチャートであり、

図９は、図８に示すステップＳＴ１のパッケージデータ生成処理について説明

するためのフローチャートである。

図10A、図10B、図10Cは、パッケージデータPf、Pjを説明するための図であり、

図11は、図8に示すステップST2の記憶領域分割装置の納入および設定処理について説明するためのフローチャートである。

図12は、1次発行データを説明するための図であり、

図13は、図8に示すステップST3の記憶領域分割装置14の設定処理の続きを説明するためのフローチャートであり、

図14Aは、領域コード取得要求を説明するための図であり、

図14Bは、装置コードリストを説明するための図であり、

図14Cは、領域管理コードリストを説明するための図であり、

図15Aは、登録可能システムコードリストを説明するための図であり、

図15Bは、領域登録許可データを説明するための図であり、

図16は、図8に示すステップST3の終了後における記憶領域分割装置の記憶部に記憶されるデータを説明するための図であり、

図17は、図8に示すステップST4の運用ファイル登録装置の設定処理の続きを説明するための図であり、

図18は、図8に示すステップST4終了後における運用ファイル登録装置に記憶されるデータを説明するための図であり、

図19A、図19Bは、ファイル登録許可データを説明するための図であり、

図20は、図8に示すステップST5で行われる記憶領域分割装置によるICカードの記憶領域分割処理を説明するためのフローチャートであり、

図21は、図20の続きのフローチャートであり、

ードの記憶領域分割処理を説明するための図であり、

図22は、ICカードの記憶領域を分割した後の状態を説明するための図であ

り、

図 2 3 は、I C カードの記憶領域に領域 A R E A を規定した後の状態を説明するための図であり、

図 2 4 は、図 8 に示すステップ S T 6 で行われる運用ファイル登録装置による I C カードへのファイルデータの登録処理を説明するための図であり、

図 2 5 は、ファイルデータの登録後の I C カードの記憶領域を説明するための図であり、

図 2 6 は、本発明の実施形態に関連付けて説明される I C I C カードシステムにおけるメモリ空間の分割の説明に供するブロック図であり、

図 2 7 は、図 2 6 に示す I C カードシステムを示すブロック図であり、

図 2 8 は、図 2 6 に示す I C カードのメモリ空間の説明に供する略線図であり、

図 2 9 は、分割後のメモリ空間を示す略線図であり、

図 3 0 は、図 2 6 に示す I C カードシステムにおいて拒絶の処理の前処理の説明に供する略線図であり、

図 3 1 は、図 3 0 の処理に続く処理の説明に供する略線図であり、

図 3 2 は、図 3 1 の処理に続く処理の説明に供する略線図であり、

図 3 3 は、図 2 6 に示す I C カードシステムにおける登録の処理の説明に供する略線図である。

#### 発明を実施するための最良の形態

以下、本発明を実施するための最良の形態実施の形態を添付図面を参照して説明する。

図 1 は、本発明の実施形態に係わる通信システム 1 の全体構成図である。

図 1 に示すように、通信システム 1 は、例えば、I C カード発行者 2 1 が使用する発行者用通信装置 1 1 と、カード記憶領域運用者 2 2 が使用する運用者用通信装置 1 2 と、装置製造者 2 3 が使用する製造者用通信装置 1 3 と、カード記憶



領域使用者 24 が使用する記憶領域分割装置 14 および運用ファイル登録装置 15 とを有する。

通信システム 1 では、IC カード発行者 21 がカード所有者 26 に IC カード 16 を発行した場合に、所定の条件に基づいて、カード記憶領域使用者 24 によって提供されるサービスに係わるファイルデータを IC カード 16 に登録し、カード所有者 26 が単体の IC カード 16 を用いて、IC カード発行者 21 およびカード記憶領域使用者 24 の双方のサービスを受けることを可能にするものである。

図 1 に示すように、通信システム 1 では、発行者用通信装置 11、運用者用通信装置 12、製造者用通信装置 13、記憶領域分割装置 14 および運用ファイル登録装置 15 が、ネットワーク 17 を介して接続される。

図 1 において、IC カード発行者 21 は、IC カード 16 の発行を行う者であり、IC カード 16 を用いて自らのサービスを提供する者である。

カード記憶領域運用者 22 は、IC カード発行者 21 からの依頼を受けて、IC カード発行者 21 が発行した IC カード 16 内の記憶部（半導体メモリ）の記憶領域のうち、IC カード発行者 21 が使用しない記憶領域をカード記憶領域使用者 24 に貸し出すサービスを行う者である。

装置製造者 23 は、カード記憶領域運用者 22 から依頼を受けて、記憶領域分割装置 14 を製造し、カード記憶領域使用者 24 に納品する者である。

カード記憶領域使用者 24 は、カード記憶領域運用者 22 に依頼を行い、IC カード 16 の記憶領域を使用して自らの独自のサービスを提供する者である。

カード所有者 26 は、IC カード発行者 21 から IC カード 16 の発行を受け、IC カード発行者 21 が提供するサービスを受ける者である。カード所有者 26 は、IC カード 16 の発行後に、カード記憶領域使用者 24 が提供するサービスを受けることを希望する場合には、記憶領域分割装置 14 および運用ファイル登録装置 15 を用いて、カード記憶領域使用者 24 のサービスに係わるファイル

データをＩＣカード１６に記憶し、その後、カード記憶領域使用者２４のサービスを受けることができる。

通信システム１は、ＩＣカード発行者２１のサービスと、カード記憶領域使用者２４のサービスとを単体のＩＣカード１６を用いて提供するに当たって、ＩＣカード発行者２１およびカード記憶領域使用者２４のサービスに係わるファイルデータが記憶される記憶領域に、権限を有しない他人によって不正にデータの書き込みおよび書き換えなどが行われることを困難にする構成を有している。

なお、図１では、それぞれ単数のＩＣカード発行者２１、カード記憶領域使用者２４およびカード所有者２６がある場合を例示したが、これらは、それぞれ複数であってもよい。

また、本実施形態の構成要素と、請求項の構成要素との対応は、例えば、ＩＣカード発行者２１および発行者用通信装置１１が本発明の第１のサービス提供元に対応している。また、カード記憶領域使用者２４が本発明の第２のサービス提供元に対応している。運用者用通信装置１２およびカード記憶領域運用者２２が本発明の記憶領域運用元に対応している。

また、領域管理鍵データＫ＿ＡＭ＿（ｉ）が本発明の第１の領域管理鍵データに対応し、領域管理鍵データＫ＿ＡＭ＿Ｆが本発明の第２の領域管理鍵データに対応している。

また、ＩＣカード１６が本発明の集積回路を搭載した携帯装置に対応している。

なお、本実施形態では、本発明の携帯装置の一例としてＩＣカード１６を例示するが、本発明の携帯装置は、例えば、ＩＣ（集積回路）を搭載した携帯電話装置や携帯情報端末装置などでもよい。

また、パッケージデータＰｆが本発明の第１のモジュールに対応している。また、パッケージデータＰｊが本発明の第２のモジュールに対応している。

また、最上位領域ＡＲＥＡ＿ＭＵ＿（ｉ）が本発明の第１の記憶領域に対応し

、最上位領域AREA\_\_MU\_\_Fが本発明の第2の記憶領域に対応している。また、最上位領域AREA\_\_MU\_\_Fの下層の領域AREAが本発明第3の記憶領域に対応している。

先ず、図1に示す通信システム1の各構成要素について説明する。

〔ICカード16〕

図2は、図1に示すICカード16の機能ブロック図である。

図2に示すように、ICカード16は、例えば、入出力インタフェース部31、記憶部32および処理部33を有する。

入出力インタフェース部31は、ICカード16が記憶領域分割装置14および運用ファイル登録装置15にそれぞれ装着されたときに、記憶領域分割装置14および運用ファイル登録装置15との間で、非接触方式あるいは接触方式で、データおよび要求の入出力を行うインタフェースである。

記憶部32は、例えば、半導体メモリであり、後述するように、ICカード発行者21およびカード記憶領域使用者24が提供するサービスに係わるデータ、並びにカード記憶領域運用者22による運用に係わるデータを記憶する。

処理部33は、ICカード16の機能に係わる処理を行う。

図3は、ICカード発行者21による発行後、カード記憶領域運用者22による運用処理前に、図2に示すICカード16の記憶部32に記憶されているデータを説明するための図である。

図3に示すように、記憶部32には、ICカード発行者21に割り当てられたシステムコードSYSC\_\_(i)と、システムコードSYSC\_\_(i)と対応付けられたシステム鍵データSYS\_\_K\_\_(i)とが記憶されている。

また、図3に示すように、記憶部32の記憶領域は、例えば、階層構造を有しており、最上位記憶領域AREA\_\_MU\_\_(i)を最上位として、その下層に複数の領域AREA\_\_(i)が規定されている。図3に示す領域AREAの下層にも、さらに領域AREA\_\_(i)が規定されていてもよい。

最上位記憶領域AREA\_\_MU\_\_(i)には、最上位領域管理鍵データK\_\_MU\_\_(i)が割り当てられている。

各領域AREA\_\_(i)には、それぞれ領域管理コードAMC\_\_(i)および領域管理鍵データK\_\_AM\_\_(i)が割り当てられている。

また、領域AREA\_\_(i)には、ICカード発行者21が提供するサービスに係わる処理を行う複数のファイルデータFILE\_\_(i)が設定(記憶)されている。

また、記憶部32には、各ファイルデータFILE\_\_(i)に対応付けられて、当該ファイルデータを用いて提供されるサービスに割り当てられたサービスコードSC\_\_(i)と、当該ファイルデータFILE\_\_(i)を設定する際に用いられるファイル管理鍵データK\_\_FM\_\_(i)とが記憶されている。

#### 〔発行者用通信装置11〕

図4は、図1に示す発行者用通信装置11の機能ブロック図である。

図4に示すように、発行者用通信装置11は、例えば、通信インタフェース部41、記憶部42および処理部43を有する。

発行者用通信装置11は、後述するように、図3に示すようにICカード16の記憶部32にセキュア状態(秘密状態)で記憶されたシステム鍵データSYS\_\_K\_\_(i)を用いて、運用者用通信装置12から受信したパッケージデータPfを暗号化してパッケージデータPjを生成する処理を行う。

なお、システム鍵データSYS\_\_K\_\_(i)は、ICカード発行者21のみが知り、図1に示すカード記憶領域運用者22、装置製造者23およびカード記憶領域使用者24には秘密にされている。

通信インタフェース部41は、ネットワーク17を介して、運用者用通信装置12との間でデータの送受信を行うインタフェースである。

記憶部42は、ICカード発行者21が発行したICカード16に記憶された図3に示す各種のデータを記憶している。

処理部 4 3 は、後述するように、運用者用通信装置 1 2 との間で、I C カード 1 6 の記憶部 3 2 の貸し出しに関する処理（P j の生成）を行う。

〔運用者用通信装置 1 2〕

図 5 は、図 1 に示す運用者用通信装置 1 2 の機能ブロック図である。

図 5 に示すように、運用者用通信装置 1 2 は、例えば、通信インタフェース部 5 1、記憶部 5 2 および処理部 5 3 を有する。

運用者用通信装置 1 2 は、I C カード 1 6 の記憶部 3 2 の記憶領域をカード記憶領域使用者 2 4 に貸し出すための種々の処理を管理する。

通信インタフェース部 5 1 は、ネットワーク 1 7 を介して、発行者用通信装置 1 1、記憶領域分割装置 1 4 および運用ファイル登録装置 1 5 との間でデータの送受信を行うインタフェースである。

記憶部 5 2 は、I C カード 1 6 の記憶部 3 2 の記憶領域を分割して形成する新たな記憶領域に関するシステムコード SYSC\_\_F と、システムコード SYSC\_\_F と対応付けられたシステム鍵データ SYS\_\_K\_\_Fなどを記憶している。

また、記憶部 5 2 は、分割用鍵データ K\_\_D を記憶している。

処理部 5 3 は、後述するように、I C カード 1 6 の記憶部 3 2 の記憶領域をカード記憶領域使用者 2 4 に貸し出すための種々の処理を行う。

〔記憶領域分割装置 1 4〕

図 6 は、図 1 に示す記憶領域分割装置 1 4 の機能ブロック図である。

記憶領域分割装置 1 4 は、例えば、カード記憶領域使用者 2 4 の店舗などに設置される。なお、記憶領域分割装置 1 4 は、運用者用通信装置 1 2 の店舗などに設置されてもよい。

また、記憶領域分割装置 1 4 は、装置製造者 2 3 によって製造され、カード記憶領域使用者 2 4 に納入される。

図 6 に示すように、記憶領域分割装置 1 4 は、例えば、通信インタフェース部 6 1、カードインタフェース部 6 2、操作部 6 3、記憶部 6 4 および処理部 6 5

を有する。

通信インタフェース部 61 は、ネットワーク 17 を介して、運用者用通信装置 12 との間でデータの送受信を行うインタフェースである。

カードインタフェース部 62 は、IC カード 16 が記憶領域分割装置 14 に装着されたときに、図 2 に示す IC カード 16 の入出力インタフェース部 31 に接続され、入出力インタフェース部 31 との間でデータおよび要求の入出力を行うインタフェースである。

操作部 63 は、例えば、カード記憶領域使用者 24 の店舗に訪れたカード所有者 26 が、指示を入力するために用いられる。

記憶部 64 は、処理部 65 の処理に必要なデータを記憶する。

処理部 65 は、IC カード 16 の記憶部 32 の記憶領域を分割して、カード記憶領域使用者 24 のサービスに係わるファイルデータを書き込む記憶領域を形成するための処理を行う。

#### 〔運用ファイル登録装置 15〕

図 7 は、図 1 に示す運用ファイル登録装置 15 の機能ブロック図である。

運用ファイル登録装置 15 は、例えば、カード記憶領域使用者 24 の店舗などに設置される。

図 7 に示すように、記憶領域分割装置 14 は、例えば、通信インタフェース部 71、カードインタフェース部 72、操作部 73、記憶部 74 および処理部 75 を有する。

通信インタフェース部 71 は、ネットワーク 17 を介して、運用者用通信装置 12 との間でデータの送受信を行うインタフェースである。

カードインタフェース部 72 は、IC カード 16 が運用ファイル登録装置 15 に装着されたときに、図 2 に示す IC カード 16 の入出力インタフェース部 31 に接続され、入出力インタフェース部 31 との間でデータおよび要求の入出力を行うインタフェースである。

操作部 73 は、例えば、カード記憶領域使用者 24 の店舗に訪れたカード所有者 26 が、指示を入力するために用いられる。

記憶部 74 は、処理部 75 の処理に必要なデータを記憶する。

処理部 75 は、前述した記憶領域分割装置 14 によって分割された記憶領域に、記憶領域分割装置 14 が提供するサービスに係わる処理に用いられるファイルデータを書き込む処理を行う。

以下、図 1 に示す通信システム 1 の動作例を説明する。

先ず、図 1 に示す通信システム 1 の全体動作の概要を説明する。

図 8 は、図 1 に示す通信システム 1 の全体動作の概要を説明するためのフローチャートである。

ステップ ST 1 :

運用者用通信装置 12 において、IC カード 16 の記憶部 32 の記憶領域を分割する際に用いられるシステムコード SYSC\_F および最上位領域管理鍵データ K\_MU\_F を含むパッケージデータ P\_f が生成され、これが分割用鍵データ K\_D で暗号化された後に送信される。そして、発行者用通信装置 11 において、システム鍵データ SYS\_K\_(i) を用いて当該パッケージデータ P\_f が暗号化されてパッケージデータ P\_j が生成され、パッケージデータ P\_j が運用者用通信装置 12 に送信される。

パッケージデータ P\_j は、運用者用通信装置 12 によって保持される。

ステップ ST 2 :

装置製造者 23 からカード記憶領域使用者 24 に、記憶領域分割装置 14 が納入される。

また、運用者用通信装置 12 から記憶領域分割装置 14 に、システムコード SYSC\_(i) およびパッケージデータ P\_j などが送信され、これらが記憶領域分割装置 14 に記憶される。

ステップ ST 3 :

運用者用通信装置 1 2 から記憶領域分割装置 1 4 に、登録可能システムコードリスト R P S L および領域登録許可データ I N F \_ A R P が送信され、これらが記憶領域分割装置 1 4 に記憶される。

登録可能システムコードリスト R P S L は、記憶領域分割装置 1 4 を用いてカード記憶領域使用者 2 4 に係わるサービスのファイルデータを登録可能な I C カード 1 6 のシステムコードを含んでいる。

領域登録許可データ I N F \_ A R P は、I C カード 1 6 の記憶領域を分割して得られた新たな記憶領域内に規定する領域 A R E A \_ F を登録するために用いられる。

#### ステップ S T 4 :

運用者用通信装置 1 2 から運用ファイル登録装置 1 5 に、領域管理鍵データ K \_ A M \_ F が、セキュアな経路で提供される。

ここで、領域管理鍵データ K \_ A M \_ F は、I C カード 1 6 の記憶領域を分割して形成される新たな記憶領域内に規定する単数または複数の領域 A R E A \_ F 内にファイルデータを書き込む際に用いられる。

また、運用ファイル登録装置 1 5 内で、ファイル登録許可データ F R P が生成される。

#### ステップ S T 5 :

例えば、カード所有者 2 6 が記憶領域分割装置 1 4 に I C カード 1 6 を装着すると、記憶領域分割装置 1 4 によって、所定の処理を経て、I C カード 1 6 の記憶部 3 2 の記憶領域が分割され、I C カード発行者 2 1 によって使用される記憶領域（図 3 に示す最上位領域 A R E A \_ M U \_ ( i ) ）と、カード記憶領域使用者 2 4 によって使用される新たな記憶領域（最上位領域管理鍵データ A R E A \_ M U \_ F ）とが規定される。

#### ステップ S T 6 :

カード所有者 2 6 が、運用ファイル登録装置 1 5 に I C カード 1 6 を装着する



と、ステップST5で規定された新たな記憶領域に、ファイル登録許可データFRPを用いて、カード記憶領域使用者24が提供するサービス提供元に係わるファイルデータが書き込まれる。

これにより、カード所有者26は、単体のICカード16を用いて、ICカード発行者21およびカード記憶領域使用者24の双方のサービスを受けることができる。

以下、図8に示す各ステップをそれぞれフローチャートを用いて詳細に説明する。

#### [パッケージデータ生成処理(ST1)]

先ず、図8に示すステップST1のパッケージデータ生成処理について説明する。

図9は、当該処理を説明するためのフローチャートである。

#### ステップST21:

図1および図5に示す運用者用通信装置12の処理部53において、図10Aに示すように、ICカード16の記憶部32の記憶領域を分割して最上位領域AREA\_\_MU\_\_(i)の他に新たに形成しようとする記憶領域の最上位領域AREA\_\_MU\_\_FのシステムコードSYSC\_\_Fと、これに対応するシステム鍵データSYS\_\_K\_\_Fとを含むパッケージデータPfを生成する。

#### ステップST22:

運用者用通信装置12の処理部53において、図10Bに示すように、ステップST1で生成したパッケージデータPfを、記憶部52から読み出した分割用鍵データK\_\_Dを用いて暗号化する。

#### ステップST23:

ステップST22で生成したパッケージデータPfが、運用者用通信装置12の通信インタフェース部51およびネットワーク17を介して、発行者用通信装置11に送信される。

パッケージデータ P f は、図 4 に示す発行者用通信装置 1 1 の通信インタフェース部 4 1 で受信される。

ステップ S T 2 4 :

図 4 に示す発行者用通信装置 1 1 の処理部 4 3 は、I C カード 1 6 の記憶部 3 2 の記憶容量のうちカード記憶領域運用者 2 2 に運用を依頼する（貸し出す）記憶領域の記憶容量を規定するための分割ブロック数データと、ステップ S T 2 3 で受信したパッケージデータ P f とを含むパッケージデータ P j を生成する。

ステップ S T 2 5 :

発行者用通信装置 1 1 の処理部 4 3 は、図 1 0 C に示すように、ステップ S T 2 4 で生成したパッケージデータ P j を、記憶部 4 2 から読み出した最上位領域管理鍵データ K \_ M U \_ ( i ) で暗号化する。

ステップ S T 2 6 :

発行者用通信装置 1 1 の処理部 4 3 は、通信インタフェース部 4 1 およびネットワーク 1 7 を介して、システムコード S Y S C \_ ( i ) 、拒絶情報 R I \_ ( i ) 、並びにステップ S T 2 5 で暗号化されたパッケージデータ P j を運用者用通信装置 1 2 に送信する。

これらは、図 5 に示す運用者用通信装置 1 2 の通信インタフェース部 5 1 で受信される。

ここで、拒絶情報 R I \_ ( i ) は、I C カード発行者 2 1 が同じ I C カード 1 6 を用いてサービスを提供することを拒絶する相手を特定するための情報である。

ステップ S T 2 7 :

図 5 に示す運用者用通信装置 1 2 の処理部 5 3 は、ステップ S T 2 6 で受信したシステムコード S Y S C \_ ( i ) 、拒絶情報 R I \_ ( i ) 、並びに暗号化されたパッケージデータ P j を記憶部 5 2 に書き込む。

〔記憶領域分割装置 1 4 の納入および設定処理 ( S T 2 ) 〕

次に、図 8 に示すステップ S T 2 の記憶領域分割装置 1 4 の納入および設定処理について説明する。

図 1 1 は、当該処理を説明するためのフローチャートである。

ステップ S T 3 1 :

カード記憶領域使用者 2 4 がカード記憶領域運用者 2 2 に、記憶領域分割装置 1 4 の発注を行う。

ステップ S T 3 2 :

カード記憶領域運用者 2 2 は、ステップ S T 3 1 で発注を受けると、カード記憶領域使用者 2 4 に納入する記憶領域分割装置 1 4 に装置コード A C (登録機コード) を発行し、これをカード記憶領域使用者 2 4 に通知する。

ステップ S T 3 3 :

カード記憶領域使用者 2 4 は、ステップ S T 3 2 で通知を受けた装置コード A C を用いて、装置製造者 2 3 に記憶領域分割装置 1 4 の納入依頼を行う。

上述したステップ S T 3 1 ~ S T 3 3 は、カード記憶領域使用者 2 4 のパーソナルコンピュータ、電話および郵便などを用いて行われる。

ステップ S T 3 4 :

装置製造者 2 3 は、ステップ S T 3 3 で受けた納入依頼に従って、必要に応じて装置コード A C の正当性をカード記憶領域運用者 2 2 に問い合わせた後に、装置コード A C を記憶した記憶領域分割装置 1 4 をカード記憶領域使用者 2 4 に納入する。

ステップ S T 3 5 :

カード記憶領域運用者 2 2 は、例えば、記憶領域分割装置 1 4 の納入完了通知をカード記憶領域使用者 2 4 から受けると、図 5 に示す運用者用通信装置 1 2 の処理部 5 3 の制御に基づいて、システムコード S Y S C \_ ( i ) 、暗号化されたパッケージデータ P j および 1 次発行データ I N F \_ 1 を記憶部 5 2 から読み出し、これらを通信インタフェース部 5 1 およびネットワーク 1 7 を介して記憶領

域分割装置 1 4 に送信する。

これらのデータは、図 6 に示す記憶領域分割装置 1 4 の通信インタフェース部 6 1 で受信される。

ここで、1 次発行データ INF\_1 は、例えば、図 1 2 に示すように、最上位領域管理鍵データ K\_MU\_F と、システムコード SYSC\_F とを格納したモジュールデータを最上位領域管理鍵データ K\_MU\_F で暗号化したデータである。

ステップ ST 3 6 :

図 6 に示す記憶領域分割装置 1 4 の処理部 6 5 は、ステップ ST 3 5 で受信したシステムコード SYSC\_(i)、暗号化されたパッケージデータ P\_j および 1 次発行データ情報 INF\_1 を記憶部 6 4 に書き込む。

〔記憶領域分割装置 1 4 の設定処理の続き (ST 3)〕

次に、図 8 に示すステップ ST 3 の記憶領域分割装置 1 4 の設定処理の続きについて説明する。

図 1 3 は、当該処理を説明するためのフローチャートである。

ステップ ST 4 1 :

カード記憶領域使用者 2 4 は、図 6 に示す記憶領域分割装置 1 4 の操作部 6 3 を操作して領域管理コード取得指示を入力する。これにより、図 1 4 A に示す領域管理コード取得要求 REQ\_AMC が、通信インタフェース部 6 1 およびネットワーク 1 7 を介して、運用者用通信装置 1 2 に送信される。

当該領域管理コード取得要求は、図 5 に示す運用者用通信装置 1 2 の通信インタフェース部 5 1 で受信される。

図 1 4 A に示すように、領域管理コード取得要求 REQ\_AMC は、装置コード AC と、拒絶情報 RI\_F と、登録領域数と、各登録領域のブロック数と、サービスコード数とを対応付けて示している。

ここで、装置コード AC は、図 1 1 に示すステップ ST 3 2 でカード記憶領域

使用者 2 4 がカード記憶領域運用者 2 2 から通知を受けた装置コードである。

拒絶情報 R I \_ F は、カード記憶領域使用者 2 4 が同じ I C カード 1 6 を用いてサービスを提供することを拒絶する相手を特定するための情報である。

登録領域数は、カード記憶領域使用者 2 4 が、自らのサービスに係わるファイルデータを記憶するために使用することを希望する、I C カード 1 6 の記憶部 3 2 に分割後に規定される領域 A R E A \_ F の数である。

各登録領域のブロック数とは、領域 A R E A に割り当てられるブロックの数である。

サービスコード数は、カード記憶領域使用者 2 4 が、自らのサービスに係わるファイルデータを記憶するために使用することを希望するサービスコードの数である。

#### ステップ S T 4 2 :

図 5 に示す運用者用通信装置 1 2 の処理部 5 3 は、ステップ S T 4 1 で領域管理コード取得要求を受信すると、装置コードリスト M C L および領域管理コードリスト A C L を生成し、これらを記憶部 5 2 に記憶する。

装置コードリスト A C L は、図 1 4 B に示すように、記憶領域分割装置 1 4 に付与された装置コード A C と、当該記憶領域分割装置 1 4 によって分割される記憶領域内に規定される単数または複数の領域 A R E A に割り当てられる領域管理コード A M C \_ F (アプリケーションコード) と、ステップ S T 4 1 で受信した拒絶情報 R I \_ F とを対応付けて示している。

また、領域管理コードリスト A M C L は、図 1 4 C に示すように、図 1 4 B の装置コードリスト A C L に示される各領域管理コード A M C \_ F (アプリケーションコード) 毎に生成され、領域管理コード A M C \_ F (アプリケーション鍵) と、それに対応する領域 A R E A \_ F に対応した領域管理鍵データ K \_ A M \_ F と、当該領域 A R E A \_ F に書き込まれるファイルデータによって提供されるサービスに付与された単数または複数のサービスコード S C とを対応付けて示してい

る。

ステップST43:

図5に示す運用者用通信装置12の処理部53は、図9に示すステップST27で記憶部52に記憶した拒絶情報RI<sub>i</sub>と、ステップST41で記憶した拒絶情報RI<sub>F</sub>とに基づいて、カード記憶領域使用者24と同じICカード16を用いてサービスを提供可能なICカード発行者21を特定する。

ステップST44:

運用者用通信装置12の処理部53は、ステップST43で特定したICカード発行者21に割り当てられたシステムコードを用いて、登録可能システムコードリストRPSLを生成する。

登録可能システムコードリストRPSLは、図15Aに示すように、記憶領域分割装置14に付与された装置コードACと、ステップST43で特定された単数または複数のICカード発行者21に付与されたシステムコードSCとを対応付けて示している。

ステップST45:

運用者用通信装置12の処理部53は、ステップST42で生成した図14Cに示す領域管理コードリストAMCLを、最上位領域管理鍵データK<sub>MU</sub><sub>F</sub>で暗号化して図15Bに示す領域登録許可データINF<sub>ARP</sub>を生成する。

ステップST46:

運用者用通信装置12の処理部53は、ステップST44で生成した登録可能システムコードリストRPSLと、ステップST45で生成した領域登録許可データINF<sub>ARP</sub>とを、通信インタフェース部51およびネットワーク17を介して、記憶領域分割装置14に送信する。

これらは、図6に示す記憶領域分割装置14の通信インタフェース部61で受信される。

ステップST47:

図6に示す記憶領域分割装置14の処理部65は、ステップST46で受信した登録可能システムコードリストRPSLおよび領域登録許可データINF\_\_ARPを、記憶部64に記憶する。

上述した図8に示すステップST3までの処理を終了した段階で、記憶領域分割装置14の記憶部64には、図16に示すように、図10Cに示す暗号化されたパッケージデータPjと、図12に示す暗号化された1次発行データINF\_\_1と、図15Aに示す登録可能システムコードリストRPSLと、図15Bに示す暗号化された領域登録許可データINF\_\_ARPとが記憶されている。

#### 〔運用ファイル登録装置15の設定処理(ST4)〕

次に、図8に示すステップST4の運用ファイル登録装置15の設定処理の続きについて説明する。

図17は、当該処理を説明するためのフローチャートである。

#### ステップST51:

図5に示す運用者用通信装置12の処理部53は、図13に示すステップST42における装置コードリストACLの生成時に発行した領域管理鍵データK\_\_AM\_\_Fを、セキュアな状態で通信インタフェース部51およびネットワーク17を介して運用ファイル登録装置15に送信、あるいはその他の手段でカード記憶領域使用者24に通知する。

#### ステップST52:

運用者用通信装置12の処理部53は、上記装置コードリストACLの生成時に発行した領域管理コードAMC\_\_F、並びにサービスコードSCを、通信インタフェース部51およびネットワーク17を介して運用ファイル登録装置15に送信に送信する。

#### ステップST53:

図7に示す運用者用通信装置12の処理部53は、図19Aに示すように、ステップST52で受信した単数または複数のサービスコードSCについて、当該

サービスコードSCと、当該サービスコードSCに対応してカード記憶領域使用者24が決定したファイル管理鍵データK<sub>FM</sub>Fとを対応付けて示すファイル登録許可データFRPを生成する。

ステップST54:

図7に示す運用者用通信装置12の処理部53は、図19Bに示すように、ステップST53で生成したファイル登録許可データFRPを、ステップST51で受けた領域管理鍵データK<sub>AM</sub>Fを用いて暗号化した後に記憶部52に記憶する。

上述した図8に示すステップST4までの処理を終了した段階で、運用ファイル登録装置15の記憶部52には、図18に示すように、領域管理コードAMC<sub>F</sub>と、領域管理鍵データK<sub>AM</sub>Fと、図19Bに示す暗号化されたファイル登録許可データFRPとが記憶されている。

〔記憶領域分割装置14によるICカード16の記憶領域分割処理(ST5)〕

次に、図8に示すステップST5で行われる記憶領域分割装置14によるICカード16の記憶領域分割処理について説明する。

図20および図21は、当該処理を説明するためのフローチャートである。

ステップST61:

カード所有者26がICカード16を持参してカード記憶領域使用者24の店舗を訪れ、ICカード16を記憶領域分割装置14に装着する。

これにより、図2に示すICカード16の記憶部32に記憶されていたシステムコードSYSC<sub>(i)</sub>が読み出され、入出力インタフェース部31を介して記憶領域分割装置14に出力される。

当該システムコードSYSC<sub>(i)</sub>は、図6に示す記憶領域分割装置14のカードインタフェース部62に入力される。

ステップST62:



図6に示す記憶領域分割装置14の処理部65は、ステップST61で入力したシステムコードSYSC\_(i)に対応するパッケージデータP<sub>j</sub>および1次発行データINF\_1を記憶部64から読み出す。

ステップST63:

記憶領域分割装置14の処理部65は、ステップST62で読み出したそれぞれ暗号化されたパッケージデータP<sub>j</sub>および1次発行データINF\_1を、カードインタフェース部62を介してICカード16に出力する。

ステップST64:

図2に示すICカード16の処理部33は、先ず、最上位領域管理鍵データK\_MU\_(i)を用いて、ステップST62で入力したパッケージデータP<sub>j</sub>を復号し、当該パッケージデータP<sub>j</sub>に含まれる分割条件情報と、暗号化されたパッケージデータP<sub>f</sub>を得る。

次に、処理部33は、分割用鍵データK\_Dを用いて、パッケージデータP<sub>f</sub>を復号し、当該パッケージデータP<sub>f</sub>に含まれるシステム鍵データSYS\_K\_Fおよび最上位領域管理鍵データK\_MU\_Fを得る。

ステップST65:

ICカード16の処理部33は、システム鍵データSYS\_K\_Fおよび最上位領域管理鍵データK\_MU\_Fを用いて暗号化を行って縮退鍵データK\_A1を生成し、当該縮退鍵データK\_A1を用いて記憶領域分割装置14との間で相互認証を行い、ICカード16および記憶領域分割装置14の双方が相手方の正当性を確認すると、ステップST66の処理に進む。

上記相互認証は、例えば、記憶領域分割装置14が、システム鍵データSYS\_K\_Fおよび最上位領域管理鍵データK\_MU\_Fを用いて暗号化を行って縮退鍵データK\_A2を生成する。そして、記憶領域分割装置14が、乱数R1を発生し、その乱数R1を縮退鍵データK\_A2を用いて暗号化を行ってデータR1aを生成する。そして、記憶領域分割装置14が、乱数R1とデータR1aと

をICカード16に出力する。ICカード16は、縮退鍵データK\_\_A1を用いてデータR1aを復号したデータが、乱数R1と一致するかを検証し、一致していれば、記憶領域分割装置14が正当な相手であると認証する。また、ICカード16が発生した乱数を用いて上述した処理と逆の立場で処理を行うことで、記憶領域分割装置14が、ICカード16が正当な相手であると認証する。

ステップST66:

図2に示すICカード16の処理部33は、記憶部32の記憶領域を分割し、図22に示すように、ICカード発行者21に割り当てられた最上位領域AREA\_\_MU\_\_(i)と、カード記憶領域使用者24に割り当てられた最上位領域AREA\_\_MU\_\_Fとを形成する。

ステップST67:

ICカード16の処理部33は、ステップST64で得た最上位領域管理鍵データK\_\_MU\_\_Fを記憶部32の最上位領域AREA\_\_MU\_\_Fと対応付けて記憶(設定)する。

ステップST68:

ICカード16の処理部33は、ステップST67で記憶した最上位領域管理鍵データK\_\_MU\_\_Fを用いて、ステップST63で入力した図12に示す1次発行データINF\_\_1を復号する。

ステップST69:

ICカード16の処理部33は、ステップST68で復号して得られた1次発行データINF\_\_1に含まれるシステムコードSYSC\_\_Fを記憶部32に記憶する。

ステップST70:

記憶領域分割装置14の処理部65は、図13のステップST47で記憶部64に記憶した図15Aに示す登録可能システムコードリストRPSL内に、図20のステップST61でICカード16から受けたシステムコードSYSC\_\_(

i) が含まれているか否かを判断し、含まれていれば、カード記憶領域使用者 24 が提供するサービスに係わるデータを IC カード 16 に登録可能であると判断し、ステップ ST 71 の処理に進む。

通信システム 1 では、ステップ ST 43 および ST 44 で説明したように、IC カード発行者 21 が同じ IC カード 16 を用いてサービスを提供することを拒絶する相手を特定するための情報である拒絶情報 RI\_(i) と、カード記憶領域使用者 24 が同じ IC カード 16 を用いてサービスを提供することを拒絶する相手を特定するための情報である拒絶情報 RI\_F とに基づいて、カード記憶領域使用者 24 と同じ IC カード 16 を用いてサービスを提供可能な IC カード発行者 21 を特定し、当該特定した IC カード発行者 21 に割り当てられたシステムコードを用いて、登録可能システムコードリスト RPSL を生成している。

これにより、カード発行者 21 およびカード記憶領域使用者 24 が、望まない相手と同じ IC カード 16 を用いてサービスを提供することを回避できる。

#### ステップ ST 71 :

記憶領域分割装置 14 の処理部 65 は、ステップ ST 70 で上記登録可能であると判断した場合に、図 13 のステップ ST 47 で記憶部 64 に記憶した図 15 に示す暗号化された領域登録許可データ INF\_ARP を、カードインタフェース部 62 を介して IC カード 16 に出力する。

IC カード 16 は、当該暗号化された領域登録許可データ INF\_ARP を、図 2 に示す入出力インタフェース部 31 を介して入力する。

前述したように、領域登録許可データ INF\_ARP は、最上位領域 AREA\_MU\_F で暗号化されている。

#### ステップ ST 72 :

図 2 に示す IC カード 16 の処理部 33 は、ステップ ST 71 で入出力インタフェース部 31 を介して入力した暗号化された領域登録許可情報 INF\_RP を記憶部 64 から読み出した最上位領域管理鍵データ K\_MU\_F を用いて復号す

る。

ステップST73:

図2に示すICカード16の処理部33は、図23に示すように、ステップST66で形成した最上位領域AREA\_\_MU\_\_Fに対応付けて、ステップST72で復号した領域登録許可情報INF\_\_RP内の領域管理鍵コードAMC\_\_Fおよび領域管理鍵データK\_\_AM\_\_Fを記憶部32に記憶する。

〔運用ファイル登録装置15によるICカード16へのファイルデータの登録(ST6)〕

次に、図8に示すステップST6で行われる運用ファイル登録装置15によるICカード16へのファイルデータの登録処理について説明する。

図24は、当該処理を説明するためのフローチャートである。

ステップST81:

カード所有者26がICカード16を持参してカード記憶領域使用者24の店舗を訪れ、ICカード16を運用ファイル登録装置15に装着する。

これにより、図7に示す運用ファイル登録装置15の処理部75が、カードインタフェース部72を介して、例えばサービスコードSCあるいはシステムコードSYSC\_\_Fなどのカード記憶領域使用者24を特定するための情報を含むファイル検索要求をICカード16に出す。

ステップST82:

図2に示すICカード16の処理部33は、ステップST81で入出力インタフェース部31がファイル検索要求を受けると、当該ファイル検索要求に含まれる上記情報に基づいて、カード記憶領域使用者24に係わるサービスのファイルデータが記憶部32に記憶されているか否かを検索する。

ステップST83:

ICカード16の処理部33は、ステップST82のファイル検索によって、カード記憶領域使用者24に係わるサービスのファイルデータが記憶部32に記

憶されていないと判断すると、入出力インタフェース部 31 を介して運用ファイル登録装置 15 にファイル無しを通知する。

ステップ ST 84 :

図 7 に示す運用ファイル登録装置 15 の処理部 75 は、ステップ ST 83 でファイル無しの通知を受けると、図 17 に示すステップ ST 54 で記憶部 74 に記憶した図 19B に示す領域管理鍵データ K\_\_AM\_\_F で暗号化されたファイル登録許可データ FRP を、カードインタフェース部 72 を介して IC カード 16 に出力する。

図 2 に示す IC カード 16 は、入出力インタフェース部 31 を介して、ファイル登録許可データ FRP を入力する。

ステップ ST 85 :

図 2 に示す IC カード 16 の処理部 33 は、ステップ ST 84 で入力したファイル登録許可データ FRP を、領域管理鍵データ K\_\_AM\_\_F を用いて復号し、当該復号されたファイル登録許可データ FRP 内のファイル管理鍵データ K\_\_FM\_\_F を用いて、図 23 に示す最上位領域 AREA\_\_MU\_\_F にカード記憶領域使用者 24 のサービスに係わるファイル管理鍵データ K\_\_FM\_\_F を書き込む。これにより、最上位領域 AREA\_\_MU\_\_F は、図 25 に示すようになる。

ステップ ST 86 :

図 2 に示す IC カード 16 の処理部 33 は、ステップ ST 85 で復号されたファイル登録許可データ FRP 内のファイル管理鍵データ K\_\_FM\_\_F およびサービスコード SC を、ステップ ST 85 で書き込んだファイルデータと対応付けて記憶部 32 に書き込む。

〔課金処理〕

通信システム 1 では、例えば、図 1 に示すカード記憶領域運用者 22 が、IC カード 16 の記憶部 32 の記憶領域の貸し出しを受けたことに対して、例えば、記憶領域のブロックを単位として IC カード発行者 21 に費用を支払う。

また、カード記憶領域運用者 22 は、IC カード 16 の記憶部 32 の記憶領域の一部をカード記憶領域使用者 24 のサービスに使用させることに対して、ライセンス料、サービスコード SC 登録使用料、領域 AREA の登録料などとして、カード記憶領域使用者 24 に費用を請求する。

以上説明したように、通信システム 1 によれば、IC カード発行者 21 がカード所有者 26 に IC カード 16 を発行した場合に、所定の条件に基づいて、IC カード 16 の記憶部 32 の未使用の記憶領域に、カード記憶領域使用者 24 によって提供されるサービスに係わるファイルデータを登録することができる。

これにより、カード所有者 26 が単体の IC カード 16 を用いて、IC カード発行者 21 およびカード記憶領域使用者 24 の双方のサービスを受けることが可能になる。

また、通信システム 1 によれば、上述したように、運用者用通信装置 12 が生成した Pf を用いて発行者用通信装置 11 の処理を経てパッケージデータ Pj を生成し、これを運用者用通信装置 12 および記憶領域分割装置 14 を介して、IC カード 16 に提供し、IC カード 16 内でパッケージデータ Pj を復号することで、IC カード 16 内のカード記憶領域使用者 24 によって使用される記憶領域（最上位領域 AREA\_\_MU\_\_F）へのファイルデータの書き込みに必要とされるシステムコード SYSC\_\_F およびシステム鍵データ SYS\_\_K\_\_F を IC カード発行者 21 に対して秘密にできる。また、パッケージデータ Pj は、IC カード 16 内でシステム鍵データ SYS\_\_K\_\_(i) を用いて復号されるため、IC カード発行者 21 によって使用される記憶領域（最上位領域 AREA\_\_MU\_\_(i)）へのファイルデータの書き込みに必要とされるシステム鍵データ SYS\_\_K\_\_(i) を、カード記憶領域運用者 22 およびカード記憶領域使用者 24 に対して秘密にできる。

また、通信システム 1 によれば、最上位領域 AREA\_\_MU\_\_(i)，AREA\_\_MU\_\_F 内に領域 AREA\_\_(i)，AREA\_\_F をそれぞれ規定し、当該

領域AREA\_(i), AREA\_Fへのファイルデータの書き込みに、領域管理鍵データK\_AM\_(i), K\_AM\_Fをそれぞれ用いることで、当該記憶領域についての不正な書き込みを、さらに効果的に防止できる。

これにより、ICカード発行者21によって使用される記憶領域にカード記憶領域使用者24が不正な書き込みを行ったり、カード記憶領域使用者24によって使用される記憶領域にICカード発行者21が不正な書き込みを行うことを防止できる。

すなわち、通信システム1によれば、ICカード16の記憶領域を分割し、分割された各記憶領域についてのデータ書き込みに用いられる鍵データを、権限の無い者に秘匿にすることで、当該記憶領域への不正なアクセスを防止できる。

その結果、ICカード16の記憶領域のうち、ICカード発行者21によって使用されていない未使用の領域を、ICカード発行者21以外のカード記憶領域使用者24に安全に使用させることができ、ICカード16の利便性を高めることができる。

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、記憶領域分割装置14および運用ファイル登録装置15をカード記憶領域使用者24に納入した後に、運用者用通信装置12から記憶領域分割装置14およびカード記憶領域使用者24に、種々のデータを設定する場合を例示したが、これらの情報は、記憶領域分割装置14および運用ファイル登録装置15をカード記憶領域使用者24の納入する前に、カード記憶領域運用者22の管理に基づいて設定してもよい。

また、上述した実施形態では、記憶領域分割装置14と運用ファイル登録装置15を別の装置として構成する場合を例示したが、これらの1つの装置で実現してもよい。

また、上述した実施形態では、記憶領域分割装置14および運用ファイル登録装置15をカード記憶領域使用者24の店舗に設置する場合を例示したが、これ

らは運用者用通信装置 1 2 の店舗などに設置してもよい。

また、上述した実施形態では、記憶領域分割装置 1 4 および運用ファイル登録装置 1 5 として専用の装置を用いたが、これらの装置は、データを必要に応じて秘匿する機能を持つ装置であることを条件に、カード記憶領域使用者 2 4 のパーソナルコンピュータなどで実現してもよい。

以下、上述した通信システム 1 と関連付けられる実施の形態の IC カードシステムについて説明する。

#### (1) 実施の形態の構成 (1-1) 基本構成

図 2 7 は、本実施の形態に係る IC カードシステムの構成を示すブロック図である。

図 2 7 において、IC カード 3 A、3 B が図 1 に示す IC カード 1 6 に対応している。

また、カード提供者 2 が、図 1 に示すカード発行者 1 1 および発行者用通信装置 1 1 に対応している。

また、貸出業者 5 および管理用サーバ 5 A が、図 1 に示すカード記憶領域運用者 2 2 および運用者用通信装置 1 2 に対応している。

また、領域使用者 6 が、図 1 に示すカード記憶領域使用者 2 4 に対応している。

また、運用端末 8 が、図 1 に示す記憶領域分割装置 1 4 および運用ファイル登録装置 1 5 に対応している。

この IC カードシステム 1 0 1 では、無償で、又はユーザーによる買い取りで、カード提供者 2 が非接触型の IC カード 3 A、3 B を発行し、この IC カード 3 A、3 B を用いた提供者端末 4 A-4 N からのアクセスにより、例えばキャッシング、駅の改札業務等の処理を実行する。またこのようにして自らの業務に係るサービスに使用して余る IC カード 3 A、3 B のメモリ空間については、貸出業者 5 の管理により又は自らの管理により使用を希望する領域使用者 6 に貸し出



す。これによりこのICカードシステム101では、カード提供者だけでなく領域使用者6においても、ICカード3A、3Bにより種々のサービスを提供できるようになされている。なおICカードシステム101においては、カード提供者2、貸出業者5、領域使用者6等の管理によるコンピュータにより一連の処理が実行されるものではあるが、以下の説明においては、説明の簡略化し、また理解を容易にするために、それぞれ適宜、カード提供者2、貸出業者5、領域使用者6等を主体にしてICカードシステム101の構成を説明する。

すなわちICカードシステム101において、カード製造者7は、カード提供者2の発注によりICカード3A、3Bを製造してカード提供者2に納入する。このときカード提供者2から通知されたカードコードCcd、貸し出し業者5から通知された分割処理鍵等を記録してICカード3A、3Bを発行する。ここでカードコードCcdは、各ICカード3A、3Bに固有の識別コードであり、後述する手順によりカード提供者2により選定される。分割処理鍵は、システム領域を別途作成する処理に係る各ICカード3A、3Bに固有の鍵である。因みに、カード提供者2は、このICカード3A、3Bについて、空き領域の管理を貸出業者5に委ねる場合には、カードコードCcdを貸出業者5に通知してライセンス料を支払い、貸出業者5の承認を得てICカード3A、3Bを発行する。

これに対してカード提供者2は、このICカード3A、3Bの発行主体であり、カードコードCcdを選定してカード製造者7に通知し、カード製造者7よりICカード3A、3Bを受け取る。またカード提供者2は、ICカード3A、3Bがカード製造者7より納品されると、専用のアクセス装置であるリーダライタによりICカード3A、3Bをアクセスし、ICカード3A、3Bによりサービスを利用可能に設定する。ここでこの処理において、カード提供者2は、図278に示すように、所定の鍵を用いた暗号化したデータの送受により、ICカード3A、3Bのメモリ空間にシステム領域を設定し、また所定ブロック数(nブロック)によるユーザー領域を設定する。

カード提供者 2 は、このシステム領域にユーザー領域のアクセスに必要なデータ、システム領域の更新に必要なデータ、システム領域の記録を特定するデータ等を記録し、提供を予定するサービスに必要なファイルをユーザー領域に記録する。

すなわちカード提供者 2 は、各ファイルの記録位置、未記録領域をブロック単位で示す領域管理情報をシステム領域に記録し、この領域管理情報により外部機器より要求された所望のファイルをアクセスできるようにする。また各ファイルに対応する暗号化処理用のファイル鍵、複数ファイルによる 1 つのサービスに適用されるアプリケーション鍵、カード提供者 2 に対応する暗号化解除用の鍵である領域管理鍵、入出力する全てのデータの暗号化処理用のシステム鍵を記録する。これにより IC カード 3 A、3 B に設定されたユーザー領域の各ブロックにおいては、対応するシステム鍵、アプリケーション鍵、領域管理鍵、ファイル鍵の組み合わせにより提供者端末 4 A、4 B より入力されるデータの暗号化を解除して、所定メモリ空間に記録することができるようになされている。

またこれらシステム鍵、領域管理鍵、アプリケーション鍵、ファイル鍵の管理用の鍵としてファイル管理鍵等を記録し、このファイル管理鍵を用いたアクセスによってのみ、システム鍵等を更新し、さらにはアプリケーション鍵、ファイル鍵を登録、更新することができないようにする。

また各サービスに固有のアプリケーションコード、システム領域の記録を特定するシステムコードを記録し、アプリケーションコード、システムコードによりこの IC カード 3 A、3 B により提供する各種サービスを識別できるようにする。なお IC カード 3 A、3 B は、1 つのサービスに係るファイルが連続したブロックに記録されるように構成され、この連続したブロックの先頭ブロックのアドレスがアプリケーションコードに割り当てられるようになされ、これによりアプリケーションコードを基準にして、対応するファイルがメモリ空間に記録され、記録された後においては、領域管理情報によりアクセスできるようになされている。

る。

カード提供者 2 は、このようなシステム領域、ユーザー領域の構築により IC カード 3 A、3 B を利用可能とすると、カード利用者に有償、無償により IC カード 3 A、3 B を提供する。さらにカード提供者 2 が展開するサービスの端末装置である提供者端末 4 A、4 B より IC カード 3 A、3 B を使用したアクセスがあると、所定のサービスを展開する。

このため提供者端末 4 A、4 B は、内蔵のリーダライタにおいて、送信に供する情報を所定の搬送波により変調して内蔵のアンテナを駆動することにより、所定周期で繰り返し IC カード 3 A、3 B に呼びかけを発する。ここで IC カード 3 A がアンテナに近接して保持されることにより、この呼びかけに対する応答が IC カード 3 A により送信されると、リーダライタは、IC カード 3 A との間で相互認証の処理を実行し、IC カード 3 A との間で相互にデータ通信可能な対象であるか否か判断する。

このようにして相互認証によりデータ交換可能な対象と判断された場合、提供者端末 4 A、4 B は、システムコードを用いた呼びかけに対する IC カード 3 A、3 B の応答を検出し、これにより対応するシステム領域を有する IC カード 3 A、3 B か否か判定する。さらにシステム管理鍵、アプリケーションコードを用いた呼びかけに対する IC カード 3 A、3 B の応答を取得することにより、自己のサービスに係る IC カード 3 A、3 B か否か判定する。提供者端末 4 A、4 B は、このようにして自己のサービスに係る IC カード 3 A、3 B と判断される場合、システム鍵、領域管理鍵、アプリケーション鍵、ファイル鍵を組み合わせによる暗号化したデータの送受によりユーザー領域をアクセスし、例えば電子マネーによるサービスを展開する場合には、IC カード 3 A に記録された金額を検出し、ユーザーにより使用された金額をこの残金より減額して IC カード 3 A に記録する等の処理を実行する。またカード提供者 2 がユーザーの購入金額に対してポイントを発行すると共に、このポイントに応じた種々のサービスを展開する場合

、ユーザーが購入した金額に応じてＩＣカード３Ａに記録されたポイントを更新する等の処理を実行する。

ＩＣカード３Ａ、３Ｂは、非接触型のＩＣカードであり、内蔵のループアンテナに誘起される電力により動作を開始し、所定の信号処理回路によりこのループアンテナに誘起される高周波信号を処理することにより、リーダライタからの呼びかけを受信する。ＩＣカード３Ａ、３Ｂは、この呼びかけに対して応答を送出し、さらにこの応答に対するリーダライタからの要求により相互認証の処理を実行し、これによりリーダライタとデータ交換可能か否か判定する。

さらにリーダライタからのシステムコード、アプリケーションコードを用いた呼びかけに対して、システム領域に記録されたシステムコード、アプリケーションコードとの照合結果をリーダライタに送信し、これによりリーダライタが提供を予定するサービスに係る場合にのみ、一連の処理を実行できるようにする。

かくするにつきＩＣカード３Ａ、３Ｂは、このようにしてリーダライタにより確認が得られると、続いて入力されるシステム鍵、領域管理鍵、アプリケーション鍵、ファイル鍵を用いたアクセスに応じて、対応するファイルをアクセスし、これによりこのファイルによる一連の処理を実行する。また領域管理鍵、システム管理鍵を用いたアクセスによりシステム領域を更新してファイル記録用の領域を確保し、さらにはファイル鍵、アプリケーションコード、アプリケーション鍵等の登録を受け付けてシステム領域を更新するようになされている。

(１－２) 領域の分割 カード提供者２は、ＩＣカード３Ａ、３Ｂのメモリ空間について、未使用領域の管理権を貸出業者５に譲って、又は自己の手元に管理権を保持したまま、この貸出業者５によりＩＣカード３Ａ、３Ｂの使用を希望する領域使用者６にメモリ空間を貸し出す。これによりこのＩＣカードシステム１０１では、領域使用者６の端末装置である運用端末８によって、この領域使用者６の提供するサービスについても利用できるようになされ、これにより例えば定期券によるＩＣカード３Ａ、３Ｂで、異なる事業者の展開する電子マネー、チケッ

ト発行等のサービスについても、利用者の希望により利用できるようなされている。

かくするにつき運用端末 8 は、各領域使用者 6 の店舗等に配置され、領域使用者 6 の運用に係るサービスを提供し、さらにこのようなサービスの提供に加えて、ユーザーの操作により、領域使用者 6 等のサービスを利用可能に IC カード 3 A、3 B を設定する端末装置である。

図 26 は、このうちの未使用領域の管理権を貸出業者 5 に譲る場合における一連の処理を示すブロック図である。ここでこの実施の形態においては、図 28 に示すように、メモリ空間の空き領域を所定ブロック数だけ分割し、この分割した領域に図 27 について上述したと同様の、管理者を貸出業者に設定してなるシステム領域（以下、新システム領域と呼ぶ）を別途設定し、この新システム領域によりこの分割した領域を管理する。

このため貸出業者 5 は、カード提供者 2 により設定されたシステム領域を利用した運用端末 8 による IC カード 3 B のアクセスにより、新システム領域の形成に必要なデータを IC カード 3 A、3 B に記録する。このとき貸出業者 5 は、カード提供者 2 により許可されたブロック数により対応するユーザー領域を確保し、さらに新システム領域の秘密情報であるシステム管理鍵、領域管理鍵等についてはカード提供者 2 を含む第 3 者に秘匿されないようにし、これによりカード提供者 2 によっても、領域使用者 6 により使用されるユーザー領域をアクセスできないようにする。

このため貸出業者 5 は、具体的にユーザー領域に記録するファイルに関する情報を除いて、新システム領域を構成する情報を分割処理鍵に対応する暗号化用の鍵により暗号化してパッケージ P f を生成し、このパッケージ P f を IC カード 3 A、3 B を特定する情報と共にカード提供者 2 に送信する。なおここでこの情報にあっては、図 28 について上述したシステム領域の各種情報のうち、ファイル鍵、アプリケーション鍵、アプリケーションコード等の具体的なサービスに関

連する情報を除いた情報がシステム領域の構成に対応するフォーマットにより配列されて作成される。これにより貸出業者 5 は、新システム領域に設定する領域管理鍵、システム管理鍵等については、カード提供者 2 に秘密にして、システム領域の生成に使用する情報をカード提供者 2 に提供するようになされている。

これによりこの IC カードシステム 101 では、図 28 について説明したシステム領域の記録に対応する第 1 の端末装置である提供者端末 4 A、4 B との間で、このシステム領域に記録された暗号化解除用の鍵であるシステム鍵により暗号化を解除可能に暗号化された情報を入出力することにより、この第 1 の端末装置によりシステム領域の記録に従ってメモリ空間がアクセスされてなる IC カード 3 A、3 B について、この IC カード 3 A、3 B に記録された所定の領域分割用鍵により暗号化を解除可能に、システム領域に対応する新システム領域の情報を暗号化して暗号化情報を生成するようになされている。

カード提供者 2 は、所定のサーバーにより、このようにして通知されたパッケージ P j に対して、貸出業者に貸し出すブロックに応じてダミーデータ等付加した後、領域管理鍵、システム鍵により暗号化して暗号化情報を生成し、さらにこの暗号化情報を図 28 について上述したシステム領域の管理によりメモリ空間の連続する所定ブロックに記録するようにアプリケーションコード等、システム管理鍵等を設定して暗号化する。これによりカード提供者 2 は、貸出業者 5 に貸し出すブロックに所定のアプリケーションに係るファイルを記録する場合に提供者端末 4 A、4 B が送出するデータ列と同様の構成に係るパッケージ P j を生成し、このパッケージ P j を相互認証鍵、システムコードと共に貸出業者 5 に提供する。これによりカード提供者 2 は、自己が管理する元のシステム領域の領域管理鍵、システム管理鍵等については、貸出業者 5 に対して秘密にして、新システム領域、対応するユーザー領域を生成するパッケージ P j を相互認証鍵等と共に貸出業者 5 に提供するようになされている。

かくするにつき貸出業者 5 は、カード提供者 2 に対して領域設定に対する課金

の処理を実行してカード提供者 2 から承認が得られることを条件に、事前の処理により、課金の処理に対応する所定枚数分の領域設定処理に係るパッケージ P j を相互認証鍵等と共にカード提供者 2 より取得し、領域使用者 6 に提供する。

これに対して運用端末 8 は、事前の設定により、提供者端末 4 A、4 B と同様にして IC カード 3 B との間で新システム領域に係る相互認証の処理を実行し、ここで相互認証を得られない場合、領域使用者 6 より相互認証鍵の提供を受け、この相互認証鍵により IC カード 3 B と相互認証の処理を実行する。ここで相互認証できた場合、この IC カード 3 B においては、未だ新システム領域が設定されていない IC カードであることにより、領域使用者 6 にその旨通知する。

これにより領域使用者 6 は、パッケージ P j を運用端末 8 に送信して IC カード 3 B に対する領域の確保を指示し、運用端末 8 においては、この指示により、提供者端末 4 A、4 B の利用に係る旧のシステム領域の記録を使用して、パッケージ P j の情報を IC カード 3 B の所定領域に記録する。これによりこの IC カードシステム 101 では、IC カード 3 B に、新システム領域と対応するユーザー領域を確保するようになされている。またこのときカード提供者 2 におけるパッケージ P f の暗号化処理に対応して、IC カード 3 B の元のシステム領域に設定されたシステム鍵、領域管理鍵により暗号化を解除した後、分割処理鍵により暗号化を解除して記録し、これにより提供者端末 4 A、4 B によるシステム領域と同様の新システム領域を形成する。

またこの新システム領域に設定した各種鍵により、カード提供者 2 によってもアクセス困難にユーザー領域を設定し、これによりメモリ空間の管理を完全に貸出業者 5 に任せることができるようになされている。

これにより IC カードシステム 101 では、このようにして IC カード 3 A、3 B のメモリ空間に貸出業者 5 による新システム領域を設定してメモリ空間を分割することにより、この分割したメモリ空間についての管理権をカード提供者 2 から貸出業者 5 が譲り受けるようになされている。

これによりＩＣカードシステム１０１では、カード提供者２が提供者端末４Ａ、４Ｂを用いて元のシステム領域によるメモリ空間の管理により実行したと同様に、例えばこの貸出業者５により専用の端末装置を用いた新システム領域によるメモリ空間の管理により、この貸出業者５についても主体的にＩＣカード３Ａ、３Ｂを管理して種々のサービスを提供できるようになされている。

かくしてＩＣカードシステム１０１では、カード提供者２側における管理用のコンピュータが、旧のシステム領域に記録された領域管理鍵により暗号化を解除可能に暗号化情報であるパッケージＰｊをさらに暗号化して第２の暗号化情報であるパッケージＰｊを生成する第２の暗号化手段を構成し、運用端末８による提供者端末４Ａ、４Ｂの相互認証鍵を用いたＩＣカード３Ａ、３Ｂのアクセスにより、この運用端末８が、第１のシステム領域である旧のシステム領域の記録に対応するＩＣカード３Ａ、３Ｂのアクセスにより、パッケージＰｊをＩＣカード３Ａ、３Ｂに入力する入力手段を構成し、これらにより第１の端末装置に対応するＩＣカード３Ａ、３Ｂのアクセスにより、パッケージＰｊの暗号化をＩＣカード３Ａ、３Ｂで解除して新システム領域の情報をＩＣカード３Ａ、３Ｂのメモリ空間に記録するようになされている。

(１－３) メモリ空間の貸出 貸出業者５は、このようにしてＩＣカード３Ａ、３Ｂのメモリ空間を分割して一部の管理権を譲り受けた場合には、この分割されたメモリ空間について、又はカード提供者２が管理権を手元に保持したままにカード提供者２よりメモリ空間の貸出が委託された場合には、この委託に係るメモリ空間について、ＩＣカード３Ａ、３Ｂの使用を希望する領域使用者６にメモリ空間を貸し出す。これによりこのＩＣカードシステム１０１では、さらに種々の業種の事業者によりＩＣカード３Ａ、３Ｂを共通に使用して種々のサービスを展開できるようになされている。

この貸し出しの処理において、貸出業者５は、カード提供者２、領域使用者６が１つのＩＣカード３Ａ、３Ｂを共用したサービスの展開を望まない場合、拒絶



の処理によりメモリ空間貸し出しを制限する。これにより例えばカード提供者 2 に対して、敵対する関係にある事業者のサービスに IC カード 3 A、3 B のメモリ空間を貸し出さないようにする。また、領域使用者 6 の所望する料金に係る IC カード 3 A、3 B について、選択的に貸し出しの処理を実行し、これにより例えば貸し出しに係る料金の高い IC カード 3 A、3 B にあっては、領域使用者 6 によっては貸し出しを拒否できるようにする。

(1-3-1) サービスの登録 図 30 は、拒絶処理に当たって、この IC カードシステム 101 における事前の処理の説明に供するブロック図である。すなわち IC カードシステム 101 において、貸出業者 5 は、カード提供者 2 によるカード製造者 7 への IC カード 3 A、3 B の製造依頼時等において、貸し出しが委ねられる IC カード 3 A、3 B については、貸出条件をカードコード C c d と共にカード提供者 2 より取得する。ここで貸出の条件は、アプリケーション (A P L) の拒絶条件、領域の価格、有効期限により構成され、アプリケーションの拒絶条件は、貸し出しを拒絶する業種、業者等のサービスを特定するデータ (例えばアプリケーションコード) 等により構成され、領域の価格は、貸し出しに係る 1 つのブロックの金額を特定するデータにより構成される。また有効期限は、貸し出す期間を特定するデータにより構成される。かくするにつき、このように貸出を拒絶する場合は、例えば敵対する事業者による IC カード 3 A、3 B の使用を禁止する場合等が考えられる。

貸出業者 5 は、このようにして取得したカードコード C c d、貸出条件を管理用サーバー 5 A に記録し、これにより IC カード 3 A、3 B 等について、カードコード C c d、貸出条件を記録してなるカードコードリストを作成する。さらにカード製造者 7 からのアクセスに対して、カードコード C c d を承認する。

さらに貸出業者 5 は、IC カード 3 A、3 B の利用を希望する領域使用者 6 に対して、運用端末 8 を設置させ、この運用端末 8 を登録機として機能させて領域使用者 6 によるサービスを登録可能とし、さらにその後この運用端末 8 により領

領域使用者 6 が IC カード 3 A、3 B をアクセスして種々のサービスに利用できるようにする。

貸出業者 5 は、各運用端末 8 により登録するサービスの情報を管理用サーバー 5 A に記録して図 3 1 に示す登録機コードリスト、アプリケーションコードリストを生成し、これらのリストとカードコードリストとを比較して実行される判定により拒絶の処理を実行する。

すなわち貸出業者 5 は、領域使用者 6 との契約により領域使用者 6 に IC カード 3 A、3 B の使用を許可した場合、領域使用者 6 から運用端末 8 に固有のコードである登録機コード M c d の発行要求があると、未使用の登録機コード M c d を領域使用者 6 に発行する。管理用サーバー 5 A は、このようにして登録機コード M c d を発行すると、この登録機コード M c d に係る運用端末 8 が領域使用者 6 に係るものであることを示す事業者コード、この運用端末 8 により運用が予定されるサービスのアプリケーション (A P L) コードを記録し、これにより登録機コードリストを作成する。なお既存の運用端末 8 で新規の領域使用者 6 のサービスを開始する場合、この新規のサービスに係るアプリケーションコードの取得要求時に、対応する登録機コードの内容が更新されて対応が図られるようになっている。

IC カードシステム 1 0 1 では、このようにして貸出業者 5 から登録機コード M c d が領域使用者 6 に通知されると、登録機製造者 1 0 にこの登録機コード M c d により運用端末 8 の納入を領域使用者 6 が依頼することとなり、この場合、貸出業者 5 は、登録機製造者 1 0 からの承認要求により、この登録機コード M c d による運用端末 8 の製造を承認する。これによりこの IC カードシステム 1 0 1 では、登録機製造者 1 0 によりこの登録機コード M c d が記録して運用端末 8 が製造され、この運用端末 8 が領域使用者 6 に引き渡されることとなり、この場合にもライセンス料が徴収される。

IC カードシステム 1 0 1 では、このようにして領域使用者 6 に引き渡された

運用端末 8 について、この運用端末 8 による新規のサービスに関するアプリケーションコードの発行が領域使用者 6 から依頼されると、貸出業者 5 は、未使用のアプリケーションコードを選択して通知し、またこのアプリケーションコードにより登録機コードリストの内容を更新する。さらに契約により設定した貸し出しに係る IC カード 3 A、3 B のブロック数、この貸出業者 5 が使用を望まない IC カードの拒絶条件（カードコードの拒絶条件）等を、対応するアプリケーション鍵と共に管理用サーバー 5 A に記録し、これによりアプリケーション（APL）コードリストを作成する。なおこの図 3 1 において、カードコードの拒絶条件は、貸出業者 5 が使用を望まない IC カードのカードコードの記録であり、具体的なカードコード、使用を諦めるブロック当たりの使用料金等である。かくするにつき、このような場合は、領域使用者 6 の敵対する事業者がカード提供者 2 である場合、使用料が高い場合等が考えられる。

貸出業者 5 は、このようにしてリストを作成すると、図 3 2 に示すように、各アプリケーションコード、カードコード毎に、カードコードリストに記録の条件と、アプリケーションコードリストに記録の条件とを比較し判定し、これにより例えばカード提供者 2 が望まない領域使用者 6 によるサービスの登録の組み合わせ、領域使用者の望まない IC カード 3 A、3 B へのサービスの登録の組み合わせ等を除いて、各サービスを IC カード 3 A、3 B にそれぞれ登録するための登録許可情報を作成してリスト化する。

このとき貸出業者 5 は、運用端末 8 より登録許可情報を IC カード 3 A、3 B に送信して、IC カード 3 A、3 B に対応するアプリケーションコード、アプリケーション鍵を IC カード 3 A、3 B に記録し、対応するファイルの記録に供するブロック数を確保することができるように、登録許可情報を記録してリストを作成する。なお貸出業者 5 が単にメモリ空間の貸出業務の委託を受けている場合、このような登録許可情報の作成に必要なシステム領域に記録の領域管理情報、システム鍵、システム管理鍵については、カード提供者 2 のみが知っていること

により、アプリケーションコード、アプリケーション鍵、ブロック数の情報をカード提供者2に通知し、カード提供者2における暗号化の処理により登録情報を生成する。これに対して貸出業者が管理するシステム領域にこれらの情報を登録して、このシステム領域に対応するメモリ空間でサービスを提供する場合、このシステム領域に記録の領域管理情報、システム鍵、システム管理鍵については、貸出業者5のみが知っていることにより、貸出業者5自らの処理により登録情報を生成する。

このようにしてアプリケーション登録リストを事前に作成した状態で、運用端末8においてICカード3A、3Bとの間でデータ交換を開始すると、上述したようにICカード3A、3Bに運用端末8に係るシステム領域が形成されていない場合には、システム領域を形成した後、運用端末8において、運用端末8のサービスに係るアプリケーションコードの記録の有無が確認される。ここでこのアプリケーションコードがICカード3A、3Bに記録されていない場合、運用端末8のサービスに係るファイルがICカード3A、3Bに未だ登録されていないことになる。このとき運用端末8は、この運用端末8により複数のサービスを提供する場合には、ICカード3A、3Bにコマンドを発行してアプリケーションコードを順次読み取り、この読み取ったアプリケーションコードにより未だ登録されていないサービスを検出する。さらにICカード3A、3Bを携帯する利用者に対して、このようにして検出した未だ登録されていないサービスについての提供の有無を確認し、ここで利用者によりサービスの希望が得られると、図33に示すように、領域使用者6を介して貸出業者5に登録機コード、サービスコードを通知する。

さらにこの登録機コードによる登録機コードリストの検索結果を基準にして、アプリケーション登録リストを検索し、ここで登録可能なサービスとして登録許可情報が記録されている場合には、このアプリケーション登録リストより対応するアプリケーションの登録許可情報を運用端末8に通知する。これに対して対応

するアプリケーションの登録許可情報が登録されていない場合、この場合には先の拒絶の処理により登録が困難であることにより、運用端末 8 を介して利用者にその旨通知する。

この IC カードシステム 101 では、この登録許可情報を運用端末 8 に通知する際に、併せて領域使用者によりサービスの提供に必要なファイルの登録に使用する登録鍵 K が通知される。運用端末 8 においては、この登録許可情報により IC カード 3 B をアクセスし、サービスに係るファイル、ファイル鍵を登録できるようにする。さらに続いて領域使用者 6 より通知される登録鍵 K を用いた IC カード 3 B のアクセスにより、サービスに係るファイル、対応するファイル鍵を登録する。これによりこの IC カードシステム 101 では、領域使用者 6 が貸出業者 5 より借り受けたメモリ空間を利用して、又は領域使用者 6 がカード提供者 2 より借り受けたメモリ空間を利用して、領域使用者 6 により管理されるファイル鍵により貸し出されたメモリ空間を管理して種々のサービスを提供できるようになされている。

このようにしてサービスを提供可能とすると、運用端末 8 は、内蔵の印刷装置によりこの利用可能としたサービスを示すシールを印刷し、このシールを IC カード 3 B の利用者に提供する。これによりこの IC カードシステム 101 では、多数のサービスを IC カード 3 B に記録した場合でも、このシールを IC カード 3 B に貼り付けることにより、提供可能なサービスを利用者により確認できるようになされている。なおこのようなシールの印刷に代えて、IC カード 3 B へ直接印刷するようにしてもよい。

かくするにつき、このようにして IC カード 3 B によりサービスを提供可能とすると、貸出業者 5 は、領域使用者 6 に対して登録時の料金の徴収に係る課金の処理を実行し、またカード提供者 2 に対して登録料の支払いに係る課金の処理を実行する。さらに貸出業者 5 は、このような登録が各 IC カードのカードコード毎にリスト化されて記録に残され、この記録の定期的な集計により例えば 1 月単

位でカード利用に供する課金の処理を実行する。

なお、本発明のデータ処理方法の一連の処理は、ハードウェアにより実行することもできるが、ソフトウェア（プログラム）により実行することもできる。一連の処理をソフトウェアにより実行する場合には、当該ソフトウェアを構成するプログラムが専用のハードウェアに組み込まれているコンピュータ、または各種のプログラムをインストールすることで各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールしてもよいし、ネットワークを介してダウンロードしてもよい。

以上説明したように、本発明によれば、複数の事業者で単体のＩＣカード等を共用使用する場合に、サービス提供元のセキュリティの面を含む各種要望に対応することができるデータ処理方法およびそのシステム、携帯装置、データ処理装置およびその方法とプログラムを提供することができる。

## 請求の範囲

1. 分割用鍵データおよび第1の領域管理鍵データを記憶する集積回路であって、前記第1の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される集積回路を搭載した携帯装置が、前記記憶領域を用いてサービスを提供する第1のサービス提供元によって発行された場合に、第2のサービス提供元に前記集積回路の前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理方法であって、

前記分割用鍵データを管理する記憶領域運用元が、第2の領域管理鍵データを含む第1のモジュールデータを前記分割用鍵データで暗号化して前記第1のサービス提供元に提供し、

前記携帯装置の発行元である前記第1のサービス提供元が、前記暗号化された第1のモジュールを含む第2のモジュールデータを前記第1の領域管理鍵データを用いて暗号化して前記記憶領域運用元に提供し、

前記記憶領域運用元の管理下で、前記暗号化された第2のモジュールデータを前記集積回路に提供し、前記集積回路内で前記第1の領域管理鍵データを用いて前記第2のモジュールデータを復号し、当該復号された第2のモジュール内の前記第1のモジュールデータを前記分割鍵データを用いて復号し、当該復号によって得られた前記第2の領域管理鍵データを用いて、前記記憶領域を前記第1のサービス提供元のサービスに用いられる第1の記憶領域と前記第2のサービス提供元のサービスに用いられる第2の記憶領域とに分割する

データ処理方法。

2. 前記集積回路は、前記第1の領域管理鍵データを用いることを条件にデータの書き込みおよびデータの書き換えの少なくとも一方が許可される前記第1の記憶領域と、前記第2の領域管理鍵データを用いることを条件にデータの書き込

みおよびデータの書き換えの少なくとも一方が許可される前記第 2 の記憶領域とに、前記記憶領域を分割する

請求項 1 に記載のデータ処理方法。

3. 前記集積回路は、第 1 のシステム鍵データをさらに記憶し、前記第 1 のシステム鍵データおよび前記第 1 の領域管理鍵データを用いることを条件に、前記記憶領域へのデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可し、

前記記憶領域運用元は、第 2 のシステム鍵データをさらに含む第 1 のモジュールデータを前記分割用鍵データで暗号化して第 1 のサービス提供元に提供し、

前記第 1 のサービス提供元は、前記暗号化された第 1 のモジュールと、前記記憶領域を他のサービス提供元に分割して利用させる条件を示す分割条件情報とを含む第 2 のモジュールデータを前記第 1 の領域管理鍵データを用いて暗号化して前記記憶領域運用元に提供し、

前記集積回路内で前記第 1 の領域管理鍵データを用いて前記第 2 のモジュールデータを復号し、当該復号された第 2 のモジュール内の前記第 1 のモジュールデータを前記分割鍵データを用いて復号し、当該復号によって得られた前記第 2 のシステム鍵データ、第 2 の領域管理鍵データおよび前記分割条件情報を用いて、前記記憶領域の分割を行う

請求項 1 に記載のデータ処理方法。

4. 前記記憶領域運用元の管理下で、前記記憶領域の分割を行うための記憶領域分割装置を前記第 2 のサービス提供元に提供し、

前記記憶領域分割装置が、前記暗号化された第 2 のモジュールデータを前記集積回路に提供する

請求項 1 に記載のデータ処理方法。

5. 前記第 2 の記憶領域内に複数の第 3 の記憶領域を規定可能であり、前記複



数の第3の記憶領域の各々について当該第3の記憶領域へのデータの書き込みおよび当該第3の記憶領域内のデータの書き換えの少なくとも一方を行うために用いられる第3の領域管理鍵データが規定されている場合に、

前記記憶領域運用元は、前記第3の領域管理鍵データを前記第2の領域管理鍵データで暗号化して前記記憶領域分割装置に提供し、

前記記憶領域分割装置は、前記暗号化された第3の領域管理鍵データを前記集積回路に提供し、

前記集積回路内で、前記暗号化された第3の領域管理鍵データを前記第2の領域管理鍵データを用いて復号し、前記第2の記憶領域内に規定された前記第3の記憶領域に対応付けて、前記復号によって得られた前記第3の領域管理鍵データを記憶する

請求項2に記載のデータ処理方法。

6. 前記記憶領域運用元は、前記第3の記憶領域のそれぞれについて、当該第3の記憶領域を用いて提供されるサービスを識別するためのサービスコードを割り当て、前記第3の記憶領域を識別するための領域コードと、当該第3の記憶領域に対応した前記第3の領域管理鍵データと、当該第3の記憶領域に割り当てられた前記サービスコードとを対応付けて示す領域コードリストを生成して記憶する

請求項5に記載のデータ処理方法。

7. 前記記憶領域運用元の管理下で、前記記憶領域の分割を行うための記憶領域分割装置を前記第2のサービス提供元に提供し、

前記記憶領域分割装置が、前記暗号化された第2のモジュールデータを前記集積回路に提供し、

前記記憶領域運用元は、前記第2のシステム鍵データおよび前記第2の領域管理鍵データを用いて暗号化して得た第1の縮退鍵データを前記記憶領域分割装置に提供し、

前記集積回路内で、前記復号して得られた前記第 2 のシステム鍵データおよび前記第 2 の領域管理鍵データを用いて暗号化を行って第 2 の縮退鍵データを生成し、

前記第 1 の縮退鍵データおよび前記第 2 の縮退鍵データを用いて、前記記憶領域分割装置と前記集積回路との間で相互認証を行う

請求項 3 に記載のデータ処理方法。

8. 前記記憶領域運用元は、

運用ファイル登録装置を前記第 2 のサービス提供元に提供し、

前記第 3 の領域管理鍵データを前記運用ファイル登録装置に提供し、

前記領域コードリスト内の前記サービスコードを前記領域コードと対応付けて前記運用ファイル登録装置に提供し、

前記運用ファイル登録装置は、

前記サービスコードと、前記第 2 のサービス提供元が発行したファイル管理鍵データとを対応付けて示すファイル登録許可データを記憶し、前記第 3 の領域管理鍵データを用いて前記ファイル登録許可データを暗号化して前記集積回路に提供し、

前記集積回路内で、前記第 3 の領域管理鍵データを用いて前記ファイル登録許可データを復号し、当該復号された前記ファイル登録許可データ内の前記ファイル管理鍵データを用いて、前記第 2 のサービス提供元のサービスに係わるファイルデータを前記第 3 の記憶領域に書き込む

請求項 6 に記載のデータ処理方法。

9. 複数の前記第 1 のサービス提供元があり、前記複数の第 1 のサービス提供元のそれぞれに前記第 1 のシステム管理鍵データと、前記第 1 のサービス提供元を識別するためのシステムコードとが付与されている場合に、

前記記憶領域運用元は、

各サービス提供元が同じ集積回路を用いてサービスを提供することを拒絶

する相手を特定するための情報である拒絶情報を前記第 1 のサービス提供元および前記第 2 のサービス提供元から受け、

前記拒絶情報に基づいて、前記第 2 のサービス提供元と同じ前記集積回路でサービスを提供可能な前記第 1 のサービス提供元に付与された前記システムコードを示した登録可能システムコードリストを生成し、

当該登録可能システムコードリストを前記記憶領域分割装置に提供し、  
前記記憶領域分割装置は、

前記集積回路の前記記憶領域の分割を行う前に、当該集積回路が記憶する前記システムコードと、前記登録可能システムコードリストとに基づいて、当該集積回路の前記記憶領域の分割を行うか否かを判断する

請求項 4 に記載のデータ処理方法。

10. 前記記憶領域運用元は、前記第 1 のサービス提供元に、前記集積回路の前記第 2 の記憶領域の使用料を支払う

請求項 1 に記載のデータ処理方法。

11. 前記第 2 のサービス提供元は、前記記憶領域運用元に、前記集積回路の前記第 2 の記憶領域の使用料を支払う

請求項 1 に記載のデータ処理方法。

12. 前記携帯装置は、カードである

請求項 1 に記載のデータ処理方法。

13. 分割用鍵データおよび第 1 の領域管理鍵データを記憶する集積回路であって、前記第 1 の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される集積回路を搭載した携帯装置が、前記記憶領域を用いてサービスを提供する第 1 のサービス提供元によって発行された場合に、第 2 のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理システムであって、

前記分割用鍵データを管理する記憶領域運用元が使用する記憶領域運用処理装置と、

前記携帯装置の発行元である前記第 1 のサービス提供元が使用する第 1 のサービス提供元処理装置と、

前記第 1 のサービス提供元が使用する第 2 のサービス提供元処理装置とを有し、

前記記憶領域運用処理装置は、第 2 の領域管理鍵データを含む第 1 のモジュールデータを前記分割用鍵データで暗号化して前記第 1 のサービス提供元処理装置に送信し、

前記第 1 のサービス提供元処理装置は、受信した前記暗号化された第 1 のモジュールを含む第 2 のモジュールデータを前記第 1 の領域管理鍵データを用いて暗号化して前記記憶領域運用処理装置に送信し、

前記記憶領域運用処理装置は、受信した前記暗号化された第 2 のモジュールデータを前記集積回路に提供し、

前記集積回路は、前記第 1 の領域管理鍵データを用いて前記第 2 のモジュールデータを復号し、当該復号された第 2 のモジュール内の前記第 1 のモジュールデータを前記分割鍵データを用いて復号し、当該復号によって得られた前記第 2 の領域管理鍵データを用いて、前記記憶領域を前記第 1 のサービス提供元のサービスに用いられる第 1 の記憶領域と前記第 2 のサービス提供元のサービスに用いられる第 2 の記憶領域とに分割する

データ処理システム。

14. 前記集積回路は、前記第 1 の領域管理鍵データを用いることを条件にデータの書き込みおよびデータの書き換えの少なくとも一方が許可される前記第 1 の記憶領域と、前記第 2 の領域管理鍵データを用いることを条件にデータの書き込みおよびデータの書き換えの少なくとも一方が許可される前記第 2 の記憶領域とに、前記記憶領域を分割する

請求項 1 3 に記載のデータ処理システム。

1 5. 前記集積回路は、第 1 のシステム鍵データをさらに記憶し、前記第 1 のシステム鍵データおよび前記第 1 の領域管理鍵データを用いることを条件に、前記記憶領域へのデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可し、

前記記憶領域運用処理装置は、第 2 のシステム鍵データをさらに含む第 1 のモジュールデータを前記分割用鍵データで暗号化して第 1 のサービス提供元処理装置に提供し、

前記第 1 のサービス提供元処理装置は、前記暗号化された第 1 のモジュールと、前記記憶領域を他のサービス提供元に分割して利用させる条件を示す分割条件情報とを含む第 2 のモジュールデータを前記第 1 の領域管理鍵データを用いて暗号化して前記記憶領域運用元処理装置に提供し、

前記集積回路は、前記第 1 の領域管理鍵データを用いて前記第 2 のモジュールデータを復号し、当該復号された第 2 のモジュール内の前記第 1 のモジュールデータを前記分割鍵データを用いて復号し、当該復号によって得られた前記第 2 のシステム鍵データ、第 2 の領域管理鍵データおよび前記分割条件情報を用いて、前記記憶領域の分割を行う

請求項 1 3 に記載のデータ処理システム。

1 6. 第 1 のサービス提供元がサービスを提供するために用いられる集積回路を搭載した携帯装置であって、

前記集積回路は、

第 2 のサービス提供元に当該集積回路の記憶領域の一部を用いたサービスを提供させる処理を行う記憶領域運用元によって管理される分割用鍵データと、第 1 の領域管理鍵データとを記憶する記憶手段と、

前記記憶領域運用元が発行した第 2 の領域管理鍵データを含むモジュールであって、前記記憶領域運用元が前記分割用鍵データを用いて暗号化し、さらに

前記第 1 のサービス提供元が前記第 1 の領域管理鍵データを用いて暗号化したモジュールを入力する入力手段と、

前記分割用鍵データおよび前記第 1 の領域管理鍵データを用いて、前記入力されたモジュールを復号し、当該復号された前記モジュール内の前記第 2 の領域管理鍵データを用いて、前記記憶手段の記憶領域を第 1 の記憶領域と第 2 の記憶領域とに分割し、前記第 1 の領域管理鍵データを用いることを条件に前記第 1 の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可し、前記第 2 の領域管理鍵データを用いることを条件に前記第 2 の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可する処理手段と

を有する携帯装置。

17. 前記処理手段は、前記第 1 の領域管理鍵データを用いることを条件に当該処理手段の処理に用いられるファイルを前記第 1 の記憶領域に書き込むことを許可し、前記第 2 の領域管理鍵データを用いることを条件に当該処理手段の処理に用いられるファイルを前記第 2 の記憶領域に書き込むことを許可する

請求項 16 に記載の携帯装置。

18. 前記記憶手段は、第 1 のシステム鍵データをさらに記憶し、

前記入力手段は、第 2 のシステム鍵データをさらに含む前記モジュールを入力し、

前記処理手段は、前記復号された前記モジュール内の前記第 2 のシステム鍵データおよび前記第 2 の領域管理鍵データを用いて、前記記憶手段の記憶領域を前記第 1 の記憶領域と前記第 2 の記憶領域とに分割し、前記第 1 のシステム鍵データおよび前記第 1 の領域管理鍵データを用いることを条件に前記第 1 の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可し、前記第 2 のシステム鍵データおよび前記第 2 の領域管理鍵データを用いることを条件に前記第 2 の記憶領域へのデータ書き込みおよび記憶領域内のデ

ータの書き換えの少なくとも一方を許可する

請求項 16 に記載の携帯装置。

19. 分割用鍵データ、第1のサービス提供元を識別するためのシステムコードおよび第1の領域管理鍵データを記憶する集積回路であって、前記第1の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可される集積回路を搭載した携帯装置が、前記記憶領域を用いて第1のサービスを提供する第1のサービス提供元によって発行された場合に、第2のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理装置であって、

記憶手段と、処理手段と、入出力手段とを有し、

前記記憶手段は、

前記第1のサービス提供元および前記第2のサービス提供元によって提示された、同じ前記集積回路でサービスを提供可能なサービス提供元を特定するための拒絶情報を記憶し、

前記処理手段は、

第2の領域管理鍵データを含む第1のモジュールを前記分割用鍵データを用いて暗号化し、

前記入出力手段は、前記暗号化された第1のモジュールを前記第1のサービス提供元に提供するために出力し、前記暗号化された第1のモジュールを含み前記第1のサービス提供元において前記第1の領域管理鍵データを用いて暗号化された第2のモジュールを入力し、前記第2のモジュールを、前記集積回路の記憶領域の一部を第2のサービス提供元が利用可能となるように前記第2のサービス提供元の管理下で前記記憶領域を分割する記憶領域分割装置に提供するために出力し、

前記処理手段は、前記拒絶情報に基づいて、前記第2のサービス提供元と同じ前記集積回路でサービスを提供可能な前記第1のサービス提供元に付与され

た前記システムコードを示す登録可能システムコードリストを生成し、

前記入出力手段は、前記記憶領域分割装置に提供するために前記システムコードリストを出力する

データ処理装置。

20. 前記記憶領域分割装置によって、前記集積回路の前記記憶領域を、前記第1の領域管理鍵データを用いることを条件にデータ書き込みおよびデータ書き換えの少なくとも一方が行われることが許可される前記第1の記憶領域と、前記第2の領域管理鍵データを用いることを条件にデータ書き込みおよびデータ書き換えの少なくとも一方が行われることが許可される前記第2の記憶領域とに分割する場合に、

前記処理手段は、前記第2の記憶領域内に複数の第3の記憶領域を規定し、前記複数の第3の記憶領域の各々について当該第3の記憶領域へのデータの書き込みおよび前記第3の記憶領域内のデータの書き換えの少なくとも一方を行うために用いられる第3の領域管理鍵データを発行し、当該第3の領域管理鍵データを前記第2の領域管理鍵データで暗号化し、

前記入出力手段は、前記記憶領域分割装置に提供するために、前記暗号化した前記第3の領域管理鍵データを出力する

請求項19に記載のデータ処理装置。

21. 前記処理手段は、前記第3の記憶領域のそれぞれについて、当該第3の記憶領域を用いて提供されるサービスを識別するためのサービスコードを発行し、前記第3の記憶領域を識別するための領域コードと、当該第3の記憶領域に対応付けられた前記第3の領域管理鍵データと、当該第3の記憶領域に割り当てられた前記サービスコードとを対応付けて示す領域コードリストを生成し、

前記記憶手段は、前記領域コードリストを記憶する

請求項20に記載のデータ処理装置。

22. 前記入出力手段は、前記第2のサービス提供元のサービスに用いられるフ



ファイルデータを前記集積回路の前記第 3 の記憶領域に書き込むファイル登録装置に提供するために、前記領域コードリストに含まれる前記領域コードと前記サービスコードとを対応付けて出力する

請求項 2 1 に記載のデータ処理装置。

2 3. 分割用鍵データ、第 1 のサービス提供元を識別するためのシステムコードおよび第 1 の領域管理鍵データを記憶する集積回路であって、前記第 1 の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可される集積回路を搭載した携帯装置が、前記記憶領域を用いて第 1 のサービスを提供する第 1 のサービス提供元によって発行された場合に、第 2 のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理装置であって、

記憶手段と、入出力手段と、処理手段とを有し、

前記記憶手段は、当該データ処理装置の処理を管理する記憶領域運用元が発行した第 2 の領域管理鍵データを含むモジュールであって、前記記憶領域運用元が前記分割用鍵データを用いて暗号化し、さらに前記第 1 のサービス提供元が前記第 1 の領域管理鍵データを用いて暗号化したモジュールと、前記第 2 のサービス提供元と同じ前記集積回路でサービスを提供可能な前記第 1 のサービス提供元に付与された前記システムコードを示した登録可能システムコードリストとを記憶し、

前記入出力手段は、前記集積回路から前記システムコードを入力し、

前記処理手段は、前記入力したシステムコードが、登録可能システムコードリストに示されたものであると判断した場合に、前記入出力手段を介して前記モジュールを前記集積回路に出力する

データ処理装置。

2 4. 第 1 の領域管理鍵データを用いることを条件に第 1 のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可され

る第1の記憶領域と、第2の領域管理鍵データを用いることを条件に第2のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第2の記憶領域とを有するに集積回路の前記第2の記憶領域に前記ファイルデータを書き込む処理を行うデータ処理装置であって、

前記第2の記憶領域内に複数の第3の記憶領域が規定され、前記複数の第3の記憶領域の各々について当該第3の記憶領域へのデータの書き込みおよび当該第3の記憶領域内のデータの書き換えの少なくとも一方を行うために用いられる第3の領域管理鍵データが規定されており、前記集積回路が前記第3の領域管理鍵データを記憶している場合に、

前記第3の領域管理鍵データと、前記第2のサービスの提供者によって発行され、前記第3の記憶領域に前記ファイルデータを書き込む際に用いられ、前記第3の領域管理鍵データで暗号化されたファイル鍵データとを記憶する記憶手段と、

前記暗号化されたファイル鍵データを前記集積回路に出力する出力手段と

前記ファイル鍵データを用いて、前記集積回路の前記第2の記憶領域に、前記第2のサービスの提供に用いられるファイルデータを書き込む書き込み手段と

を有するデータ処理装置。

25. 分割用鍵データおよび第1の領域管理鍵データを記憶し、前記第1の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される集積回路を搭載した携帯物を発行し、

前記分割用鍵データを用いて、前記第1の領域管理鍵データを用いることを条件にデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される第1の記憶領域と、第2の領域管理鍵データを用いる

ことを条件にデータの書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を行うことが許可される第2の記憶領域とに前記集積回路の前記記憶領域を分割することを、前記分割用鍵データを管理する記憶領域運用元に依頼する携帯物発行方法。

## 26. 前記携帯物は、カードである

請求項25に記載の携帯物発行方法。

27. 分割用鍵データ、第1のサービス提供元を識別するためのシステムコードおよび第1の領域管理鍵データを記憶する集積回路であって、前記第1の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可される集積回路を搭載した携帯装置が、前記記憶領域を用いて第1のサービスを提供する第1のサービス提供元によって発行された場合に、第2のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理をコンピュータに実行させるプログラムであって、

前記集積回路から前記システムコードを入力する手順と、

前記第2のサービス提供元と同じ前記集積回路でサービスを提供可能な前記第1のサービス提供元に付与された前記システムコードを示した登録可能システムコードリストを参照し、前記入力したシステムコードが、前記登録可能システムコードリストに示されたものであるか否かを判断する手順と、

前記入力したシステムコードが、登録可能システムコードリストに示されたものであると判断した場合に、当該プログラムの実行を管理する記憶領域運用元が発行した第2の領域管理鍵データを含むモジュールであって、前記記憶領域運用元が前記分割用鍵データを用いて暗号化し、さらに前記第1のサービス提供元が前記第1の領域管理鍵データを用いて暗号化したモジュールを前記集積回路に出力する手順と

を前記コンピュータに実行させるプログラム。

28. 分割用鍵データ、第1のサービス提供元を識別するためのシステムコードおよび第1の領域管理鍵データを記憶する集積回路であって、前記第1の領域管理鍵データを用いることを条件に当該集積回路内の記憶領域へのデータ書き込みおよび記憶領域内のデータの書き換えの少なくとも一方を許可される集積回路を搭載した携帯装置が、前記記憶領域を用いて第1のサービスを提供する第1のサービス提供元によって発行された場合に、第2のサービス提供元に前記記憶領域の一部を用いたサービスを提供させる処理を行うデータ処理方法であって、

前記集積回路から前記システムコードを入力する手順と、

前記第2のサービス提供元と同じ前記集積回路でサービスを提供可能な前記第1のサービス提供元に付与された前記システムコードを示した登録可能システムコードリストを参照し、前記入力したシステムコードが、前記登録可能システムコードリストに示されたものであるか否かを判断する手順と、

前記入力したシステムコードが、前記登録可能システムコードリストに示されたものであると判断した場合に、当該プログラムの実行を管理する記憶領域運用元が発行した第2の領域管理鍵データを含むモジュールであって、前記記憶領域運用元が前記分割用鍵データを用いて暗号化し、さらに前記第1のサービス提供元が前記第1の領域管理鍵データを用いて暗号化したモジュールを前記集積回路に出力する手順と

を有するデータ処理方法。

29. 第1の領域管理鍵データを用いることを条件に第1のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第1の記憶領域と、第2の領域管理鍵データを用いることを条件に第2のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第2の記憶領域とを有するに集積回路の前記第2の記憶領域に前記ファイルデータを書き込む処理をコンピュータに実行させるプログラムであって、

前記第 2 の記憶領域内に複数の第 3 の記憶領域が規定され、前記複数の第 3 の記憶領域の各々について当該第 3 の記憶領域へのデータの書き込みおよび当該第 3 の記憶領域内のデータの書き換えの少なくとも一方を行うために用いられる第 3 の領域管理鍵データが規定されており、前記集積回路が前記第 3 の領域管理鍵データを記憶している場合に、

前記第 2 のサービスの提供者によって発行され、前記第 3 の記憶領域に前記ファイルデータを書き込む際に用いられ、前記第 3 の領域管理鍵データで暗号化されたファイル鍵データを、前記集積回路に出力する手順と、

前記ファイル鍵データを用いて、前記集積回路の前記第 2 の記憶領域に、前記第 2 のサービスの提供に用いられるファイルデータを書き込む手順と

を前記コンピュータに実行させるプログラム。

30. 第 1 の領域管理鍵データを用いることを条件に第 1 のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第 1 の記憶領域と、第 2 の領域管理鍵データを用いることを条件に第 2 のサービスの提供に用いられるファイルデータの書き込みおよび書き換えの少なくとも一方が許可される第 2 の記憶領域とを有するに集積回路の前記第 2 の記憶領域に前記ファイルデータを書き込む処理を行うデータ処理方法であって、

前記第 2 の記憶領域内に複数の第 3 の記憶領域が規定され、前記複数の第 3 の記憶領域の各々について当該第 3 の記憶領域へのデータの書き込みおよび当該第 3 の記憶領域内のデータの書き換えの少なくとも一方を行うために用いられる第 3 の領域管理鍵データが規定されており、前記集積回路が前記第 3 の領域管理鍵データを記憶している場合に、

前記第 2 のサービスの提供者によって発行され、前記第 3 の記憶領域に前記ファイルデータを書き込む際に用いられ、前記第 3 の領域管理鍵データで暗号化されたファイル鍵データを、前記集積回路に出力する手順と、

前記ファイル鍵データを用いて、前記集積回路の前記第 2 の記憶領域に、前

記第 2 のサービスの提供に用いられるファイルデータを書き込む手順と  
を有するデータ処理方法。

FIG. 1

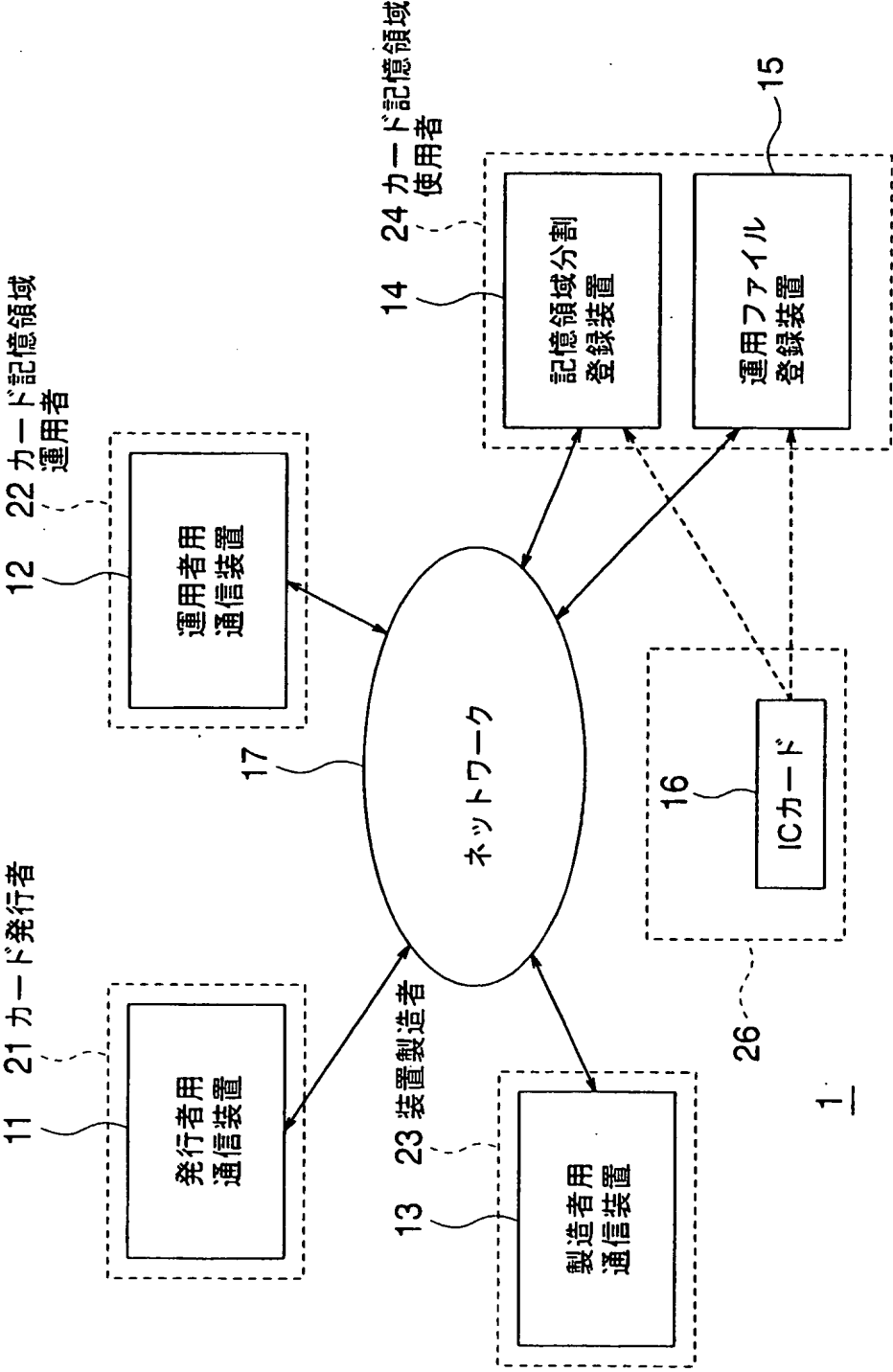


FIG. 2

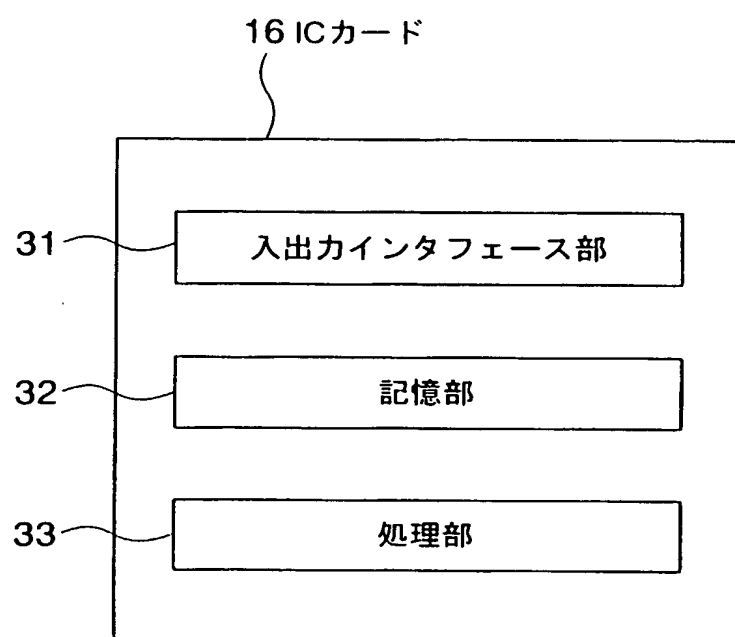




FIG. 3

32 ICカード6の記憶部

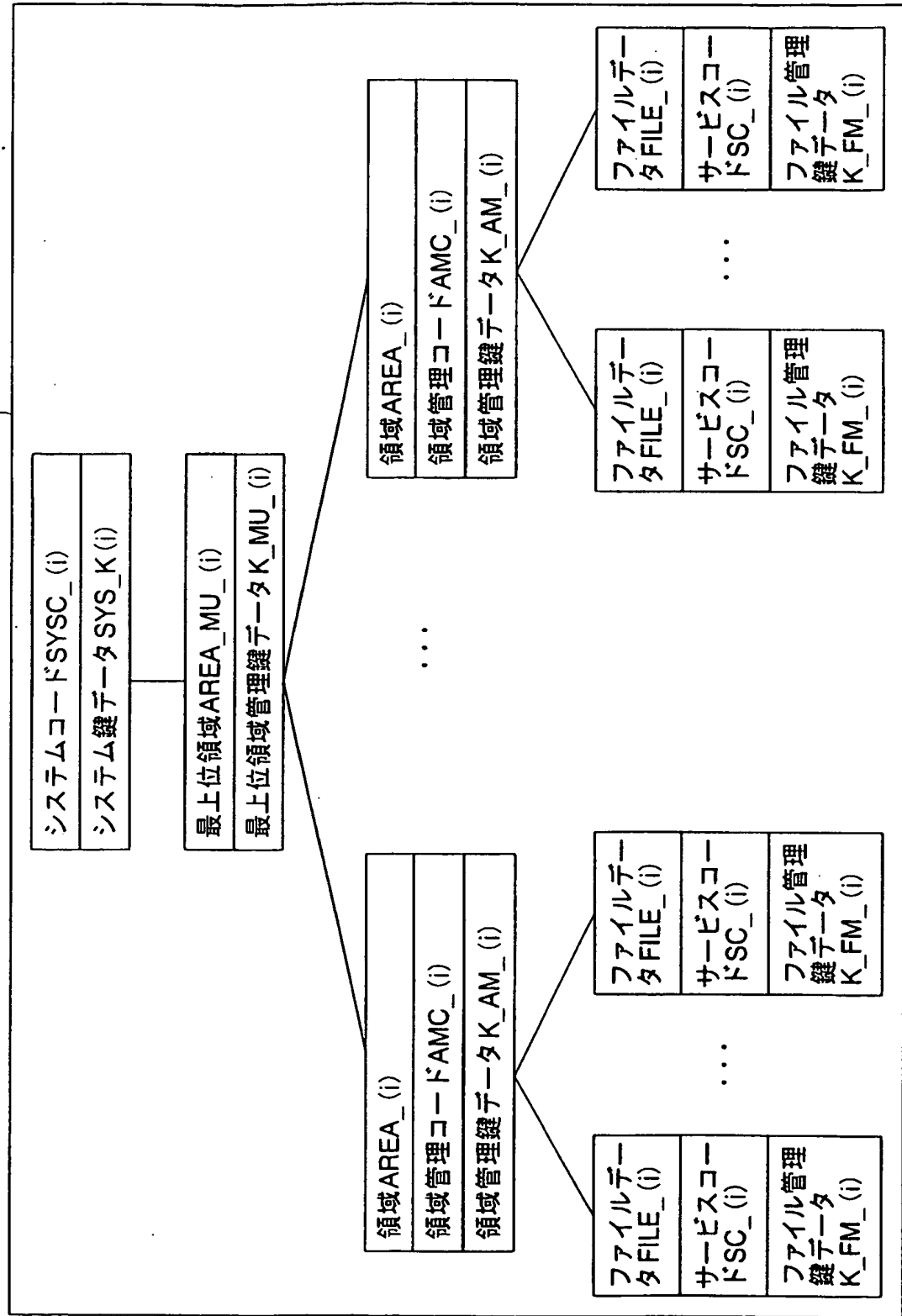


FIG. 4

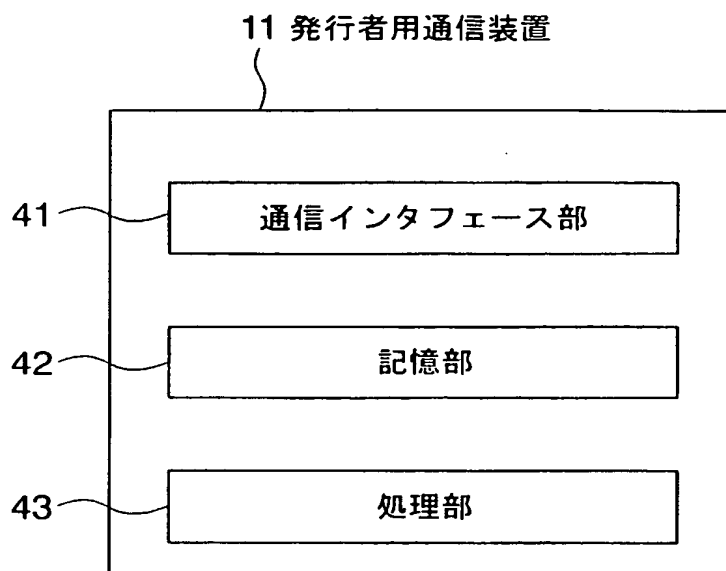


FIG. 5

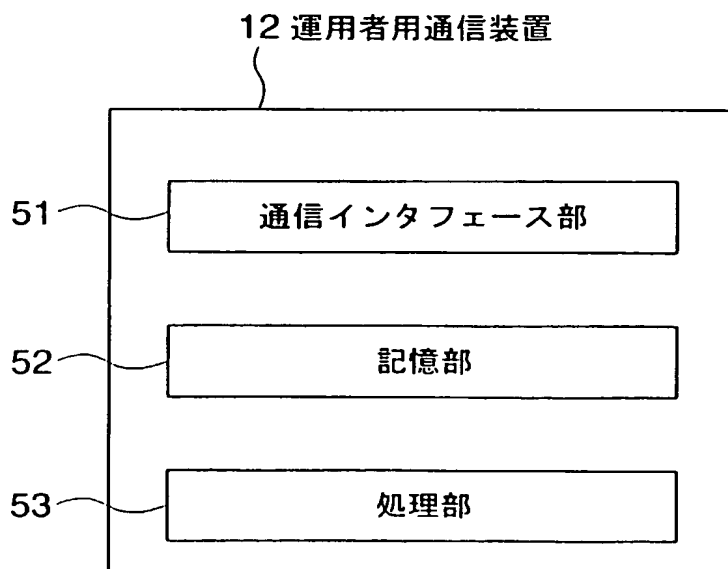


FIG. 6

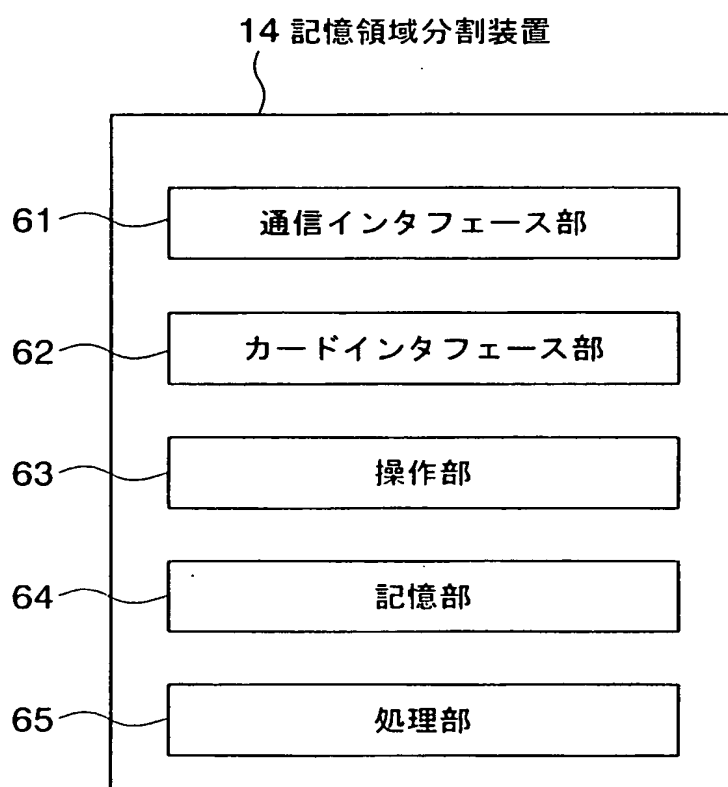


FIG. 7

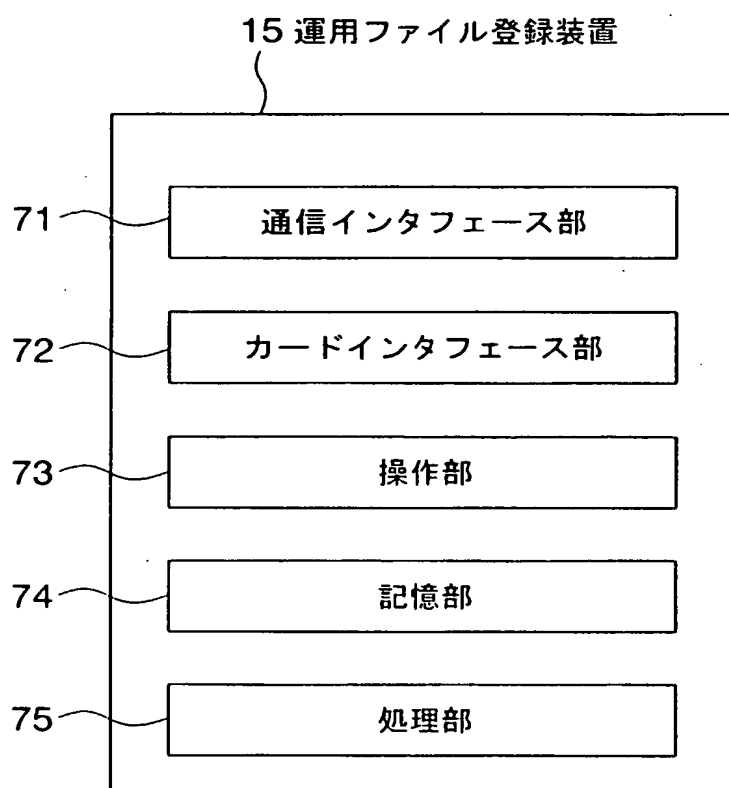


FIG. 8

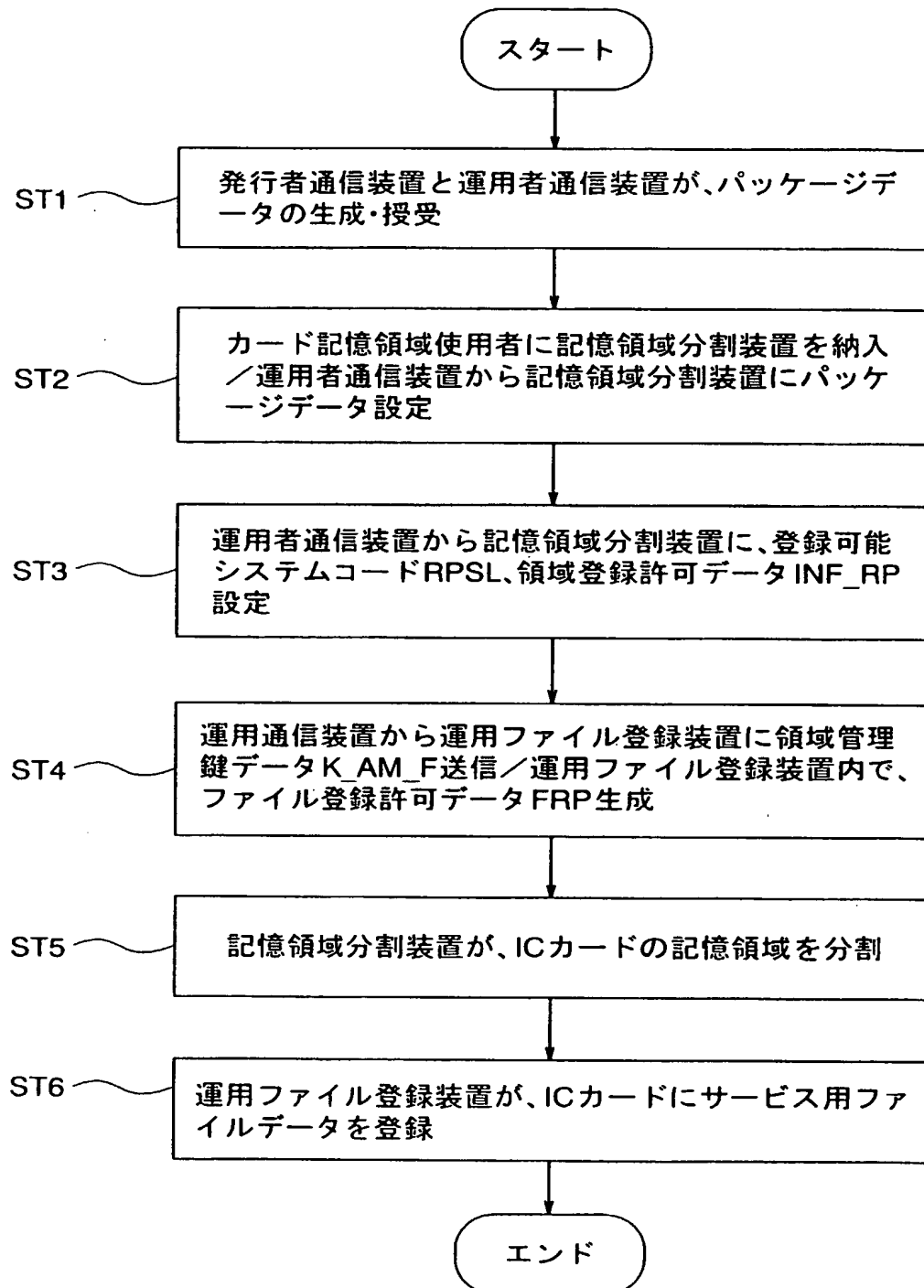


FIG. 9

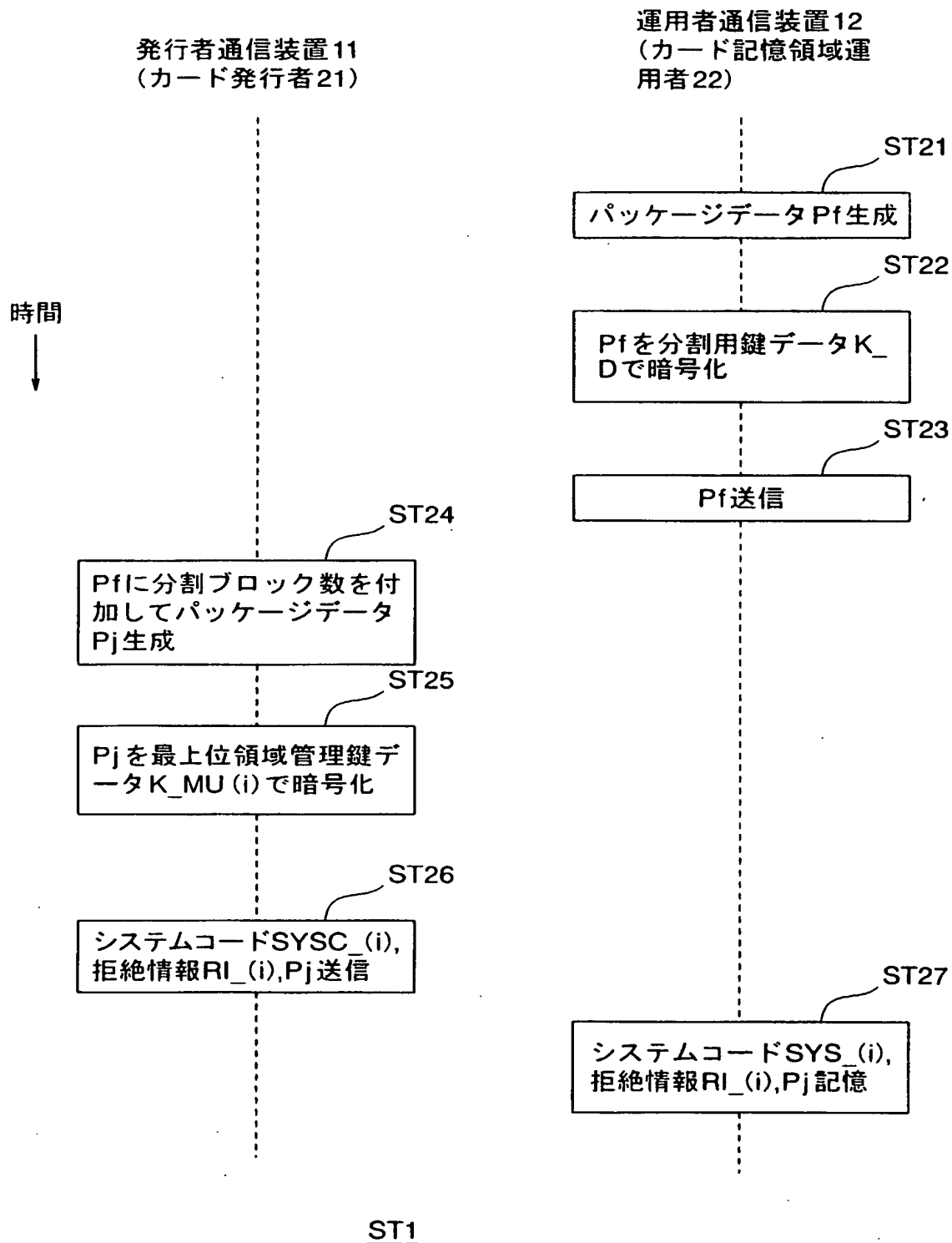
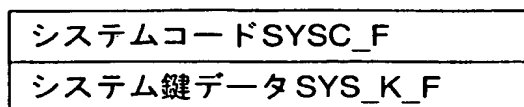
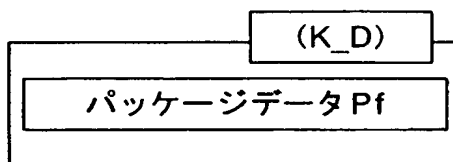


FIG. 10A



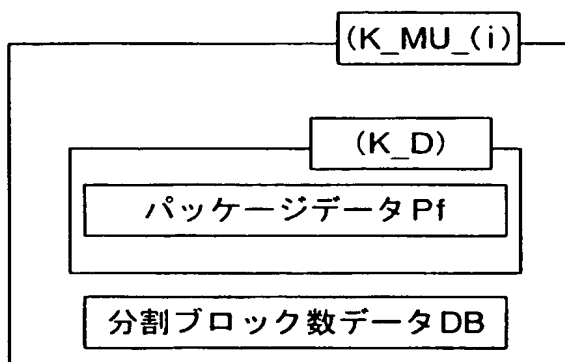
パッケージデータ Pf

FIG. 10B



K\_D: 分割用鍵データ

FIG. 10C



K\_MU\_(i)): 最上位領域管理鍵データ

パッケージデータ Pj

FIG. 11

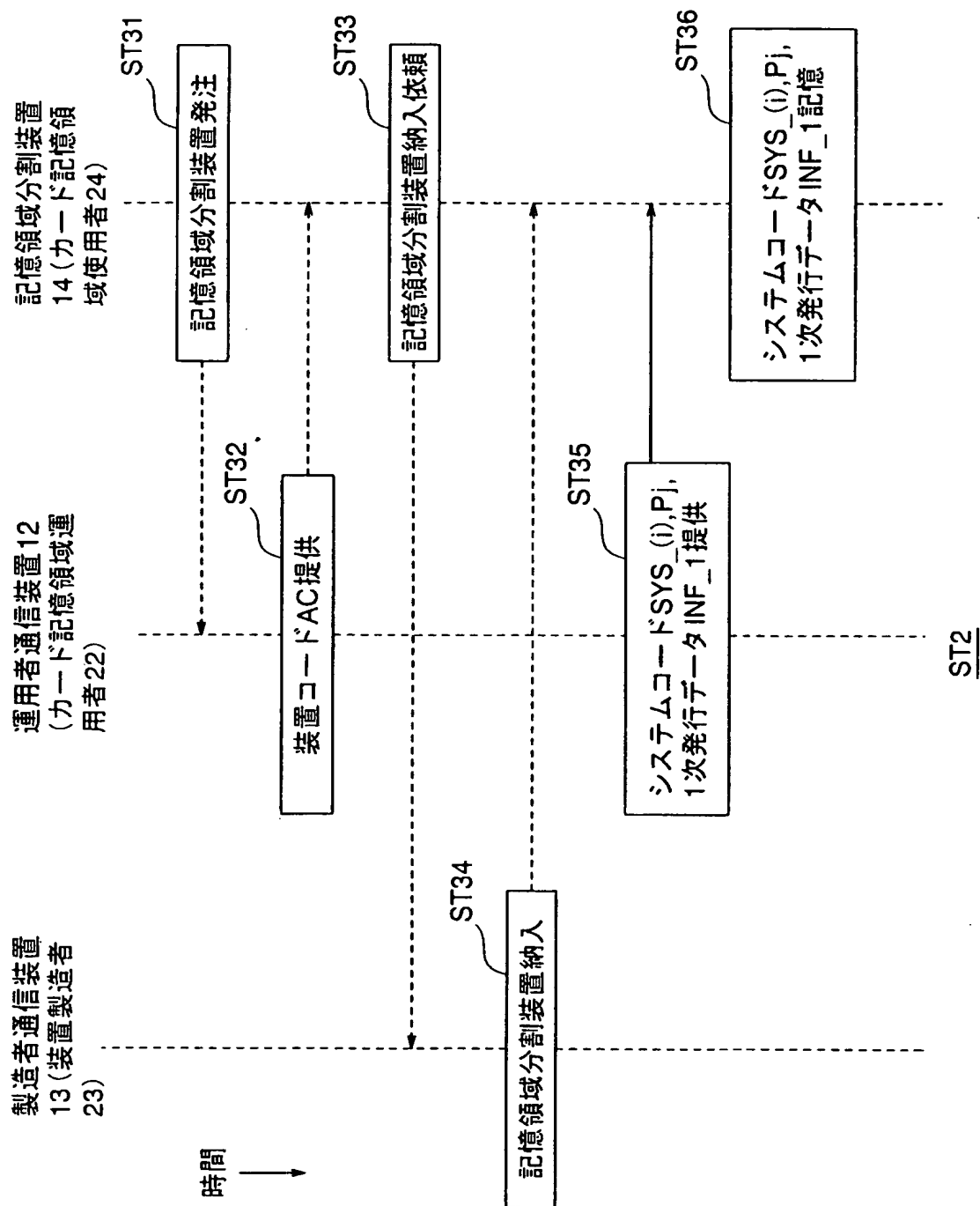
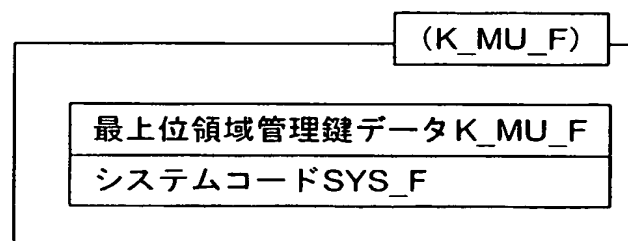




FIG. 12



1次発行データ INF\_1

FIG. 13

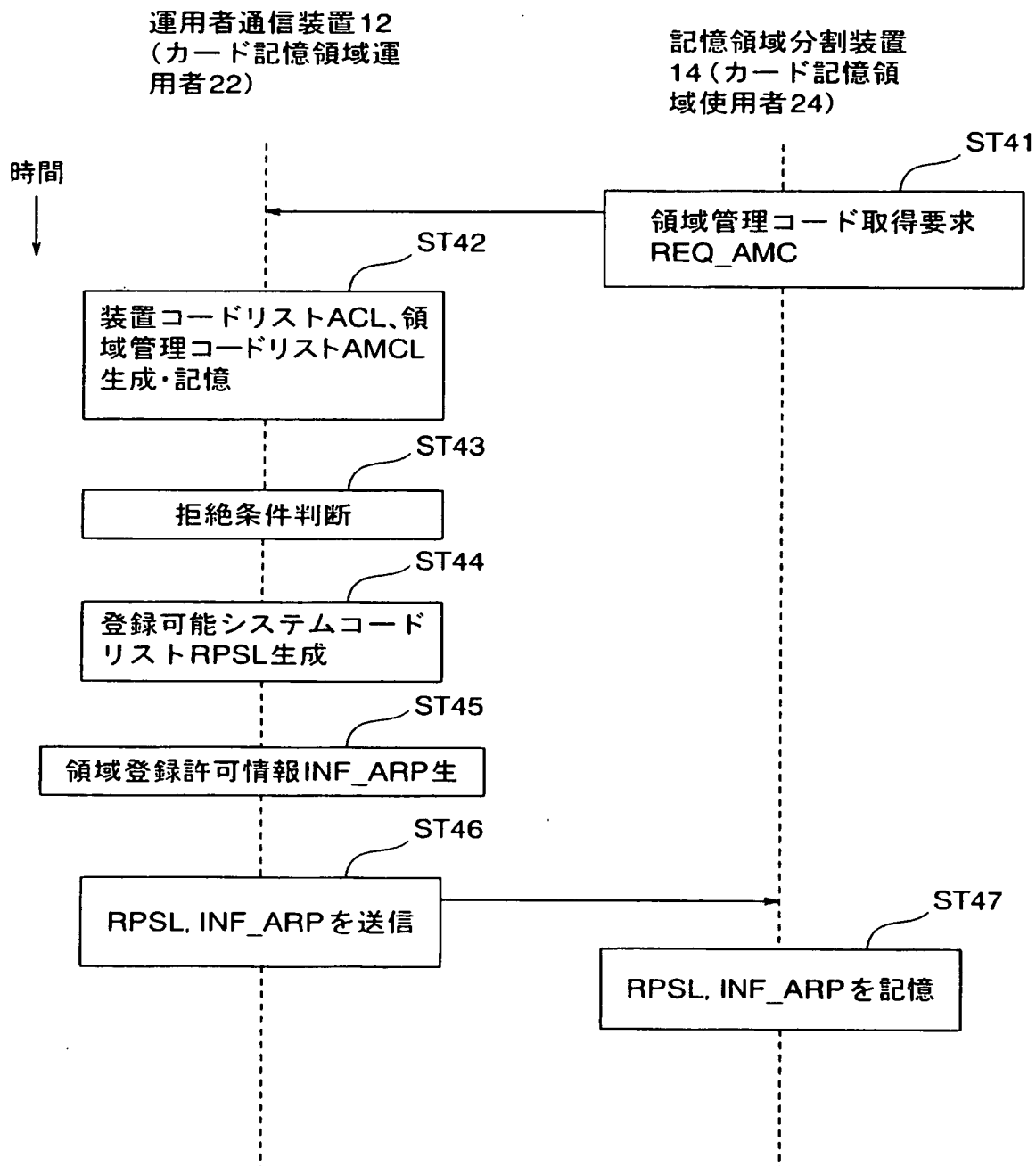
ST3

FIG. 14A

登録装置コードAC
拒絶情報RI_F
登録領域数
各登録領域のブロック数
サービスコード数

領域コード取得要求REQ\_AMC

FIG. 14B

装置コードAC
領域管理コードAMC_F
領域管理コードAMC_F
...
領域管理コードAMC_F
拒絶情報RI_F

装置コードリストACL

FIG. 14C

領域管理コードAMC_F
領域管理鍵データK_AM_F
領域ブロック数
サービスコードSC
...
サービスコードSC

領域管理コードリストAMCL

FIG. 15A

装置コードAC
システムコードSC
システムコードSC
...
システムコードSC

登録可能システムコードリストRPSL

FIG. 15B

(K_MU_F)
領域管理コードAMC_F
領域管理鍵データK_AM_F
領域ブロック数
サービスコードSC
サービスコードSC
...
サービスコードC

領域登録許可データINF\_RP

FIG. 16

記憶領域分割装置の記憶部(ST3終了時)

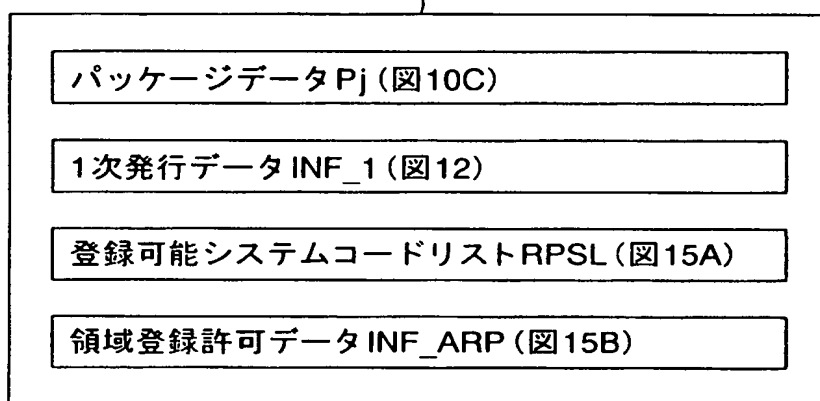


FIG. 17

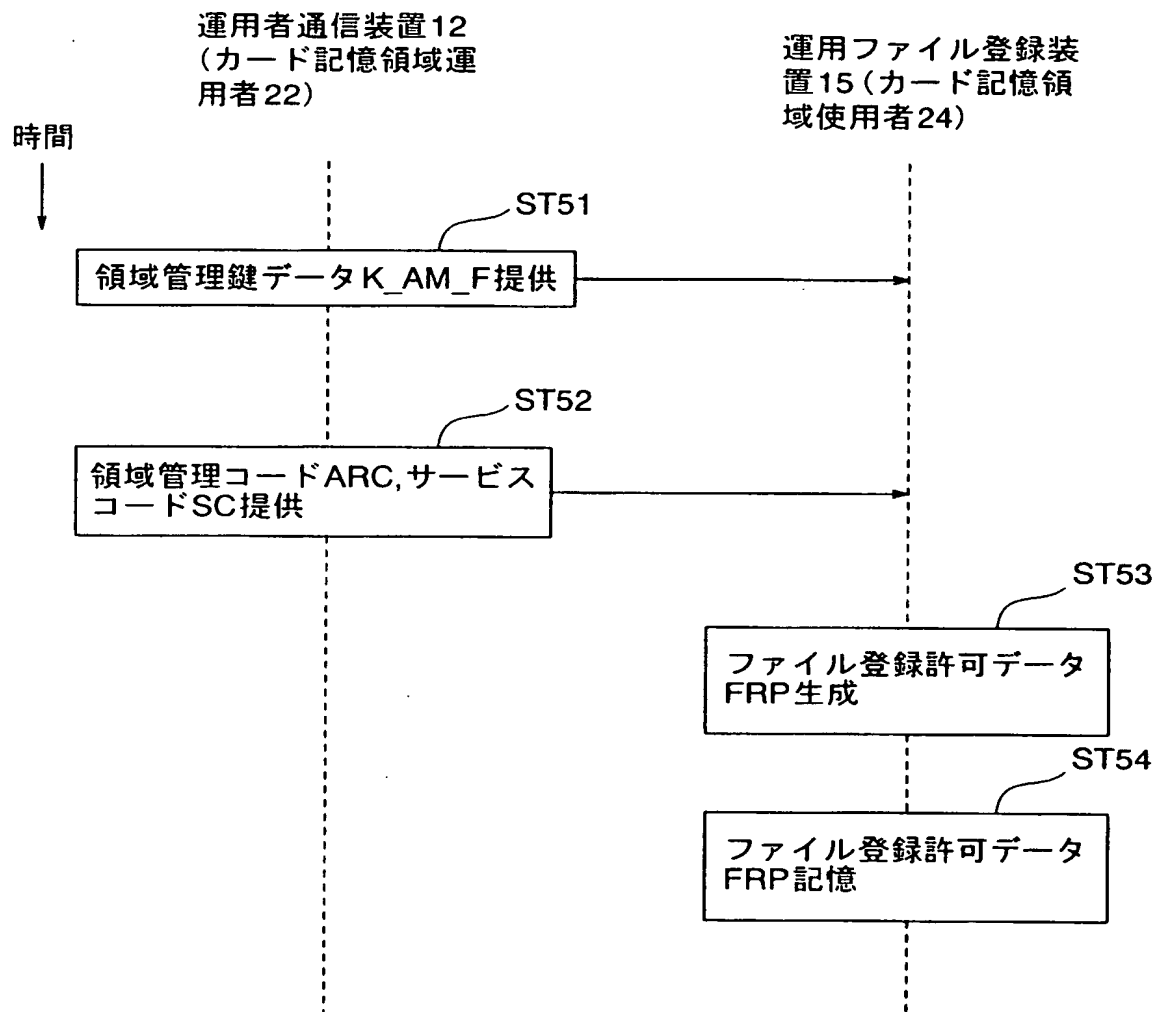


FIG. 18

運用ファイル登録装置の記憶部(ST4終了時)

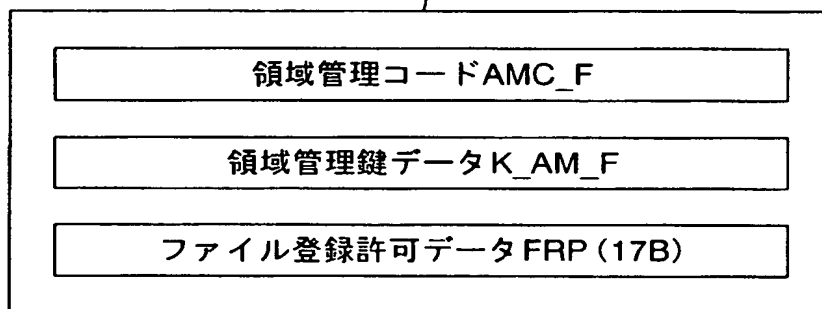
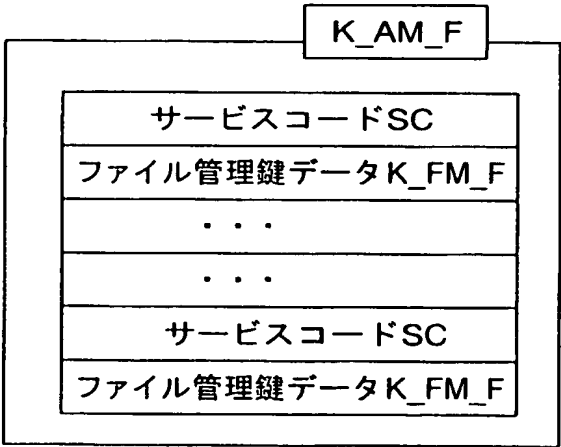


FIG. 19A

サービスコードSC
ファイル管理鍵データK_FM_F
...
...
サービスコードSC
ファイル管理鍵データK_FM_F

ファイル登録許可データFRP

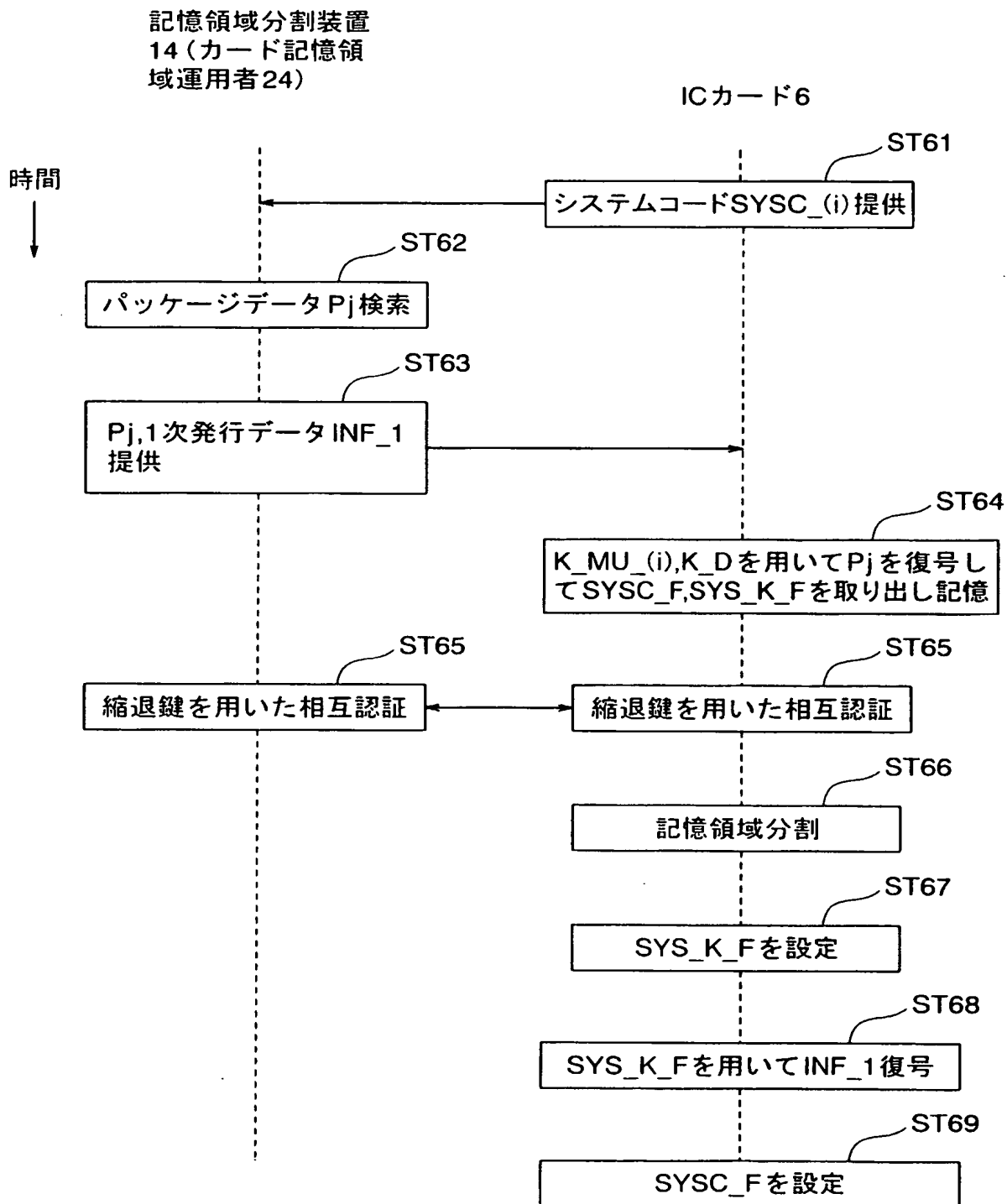
FIG. 19B



ファイル登録許可データFRP



FIG. 20



ST5

FIG. 21

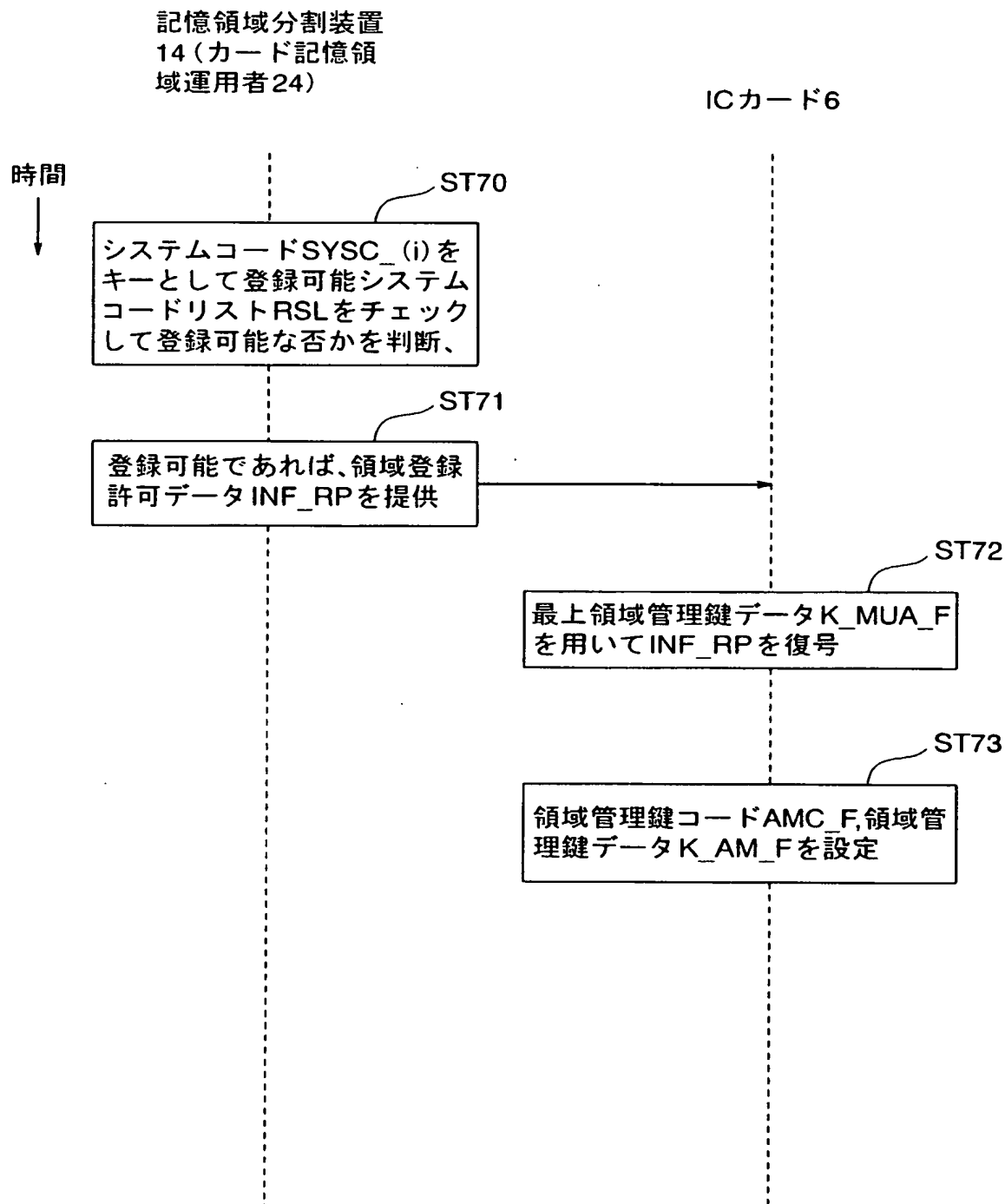
ST5

FIG. 22

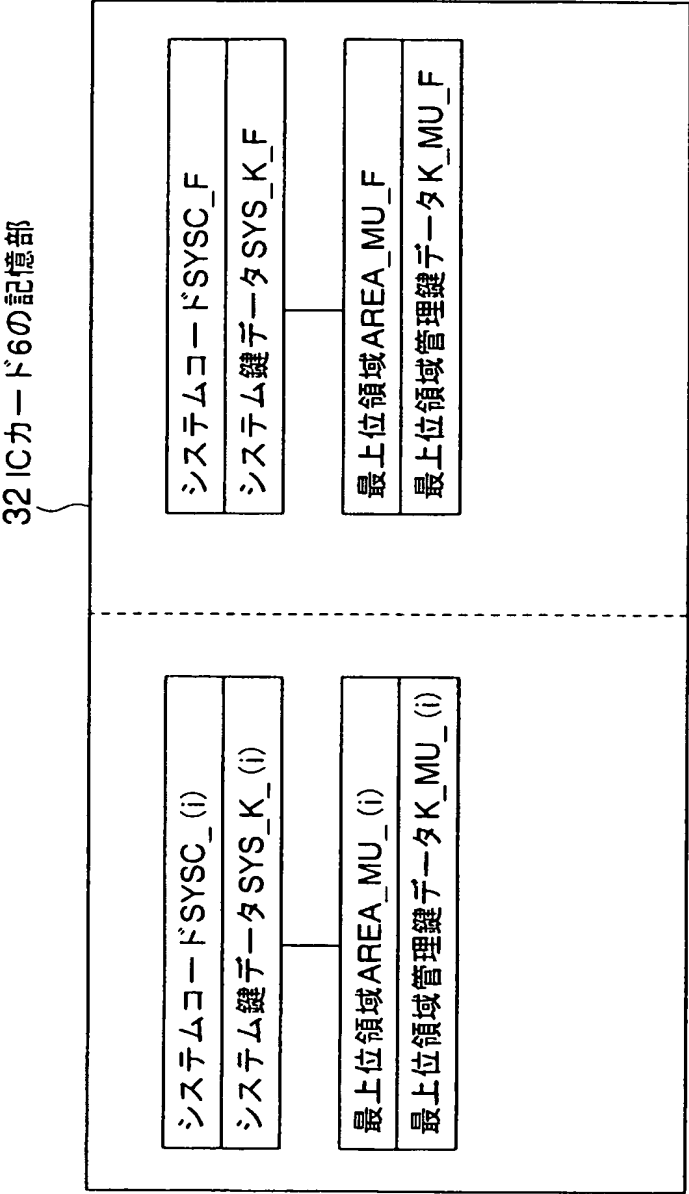
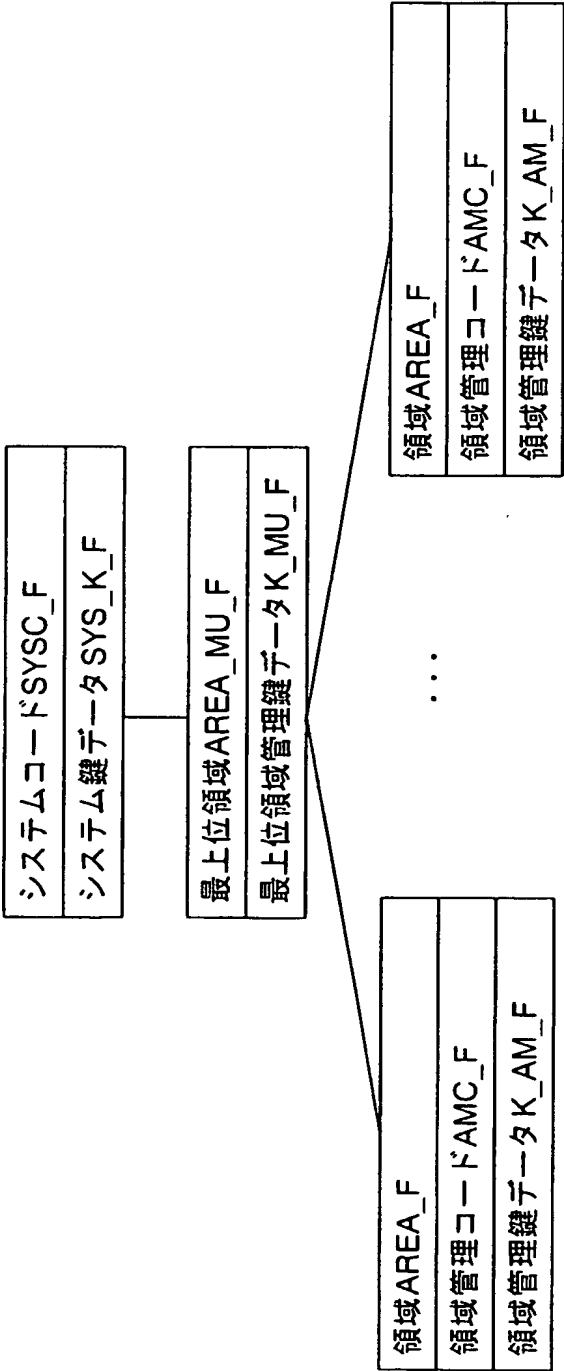


FIG. 23



最上位領域AREA\_MU\_F

FIG. 24

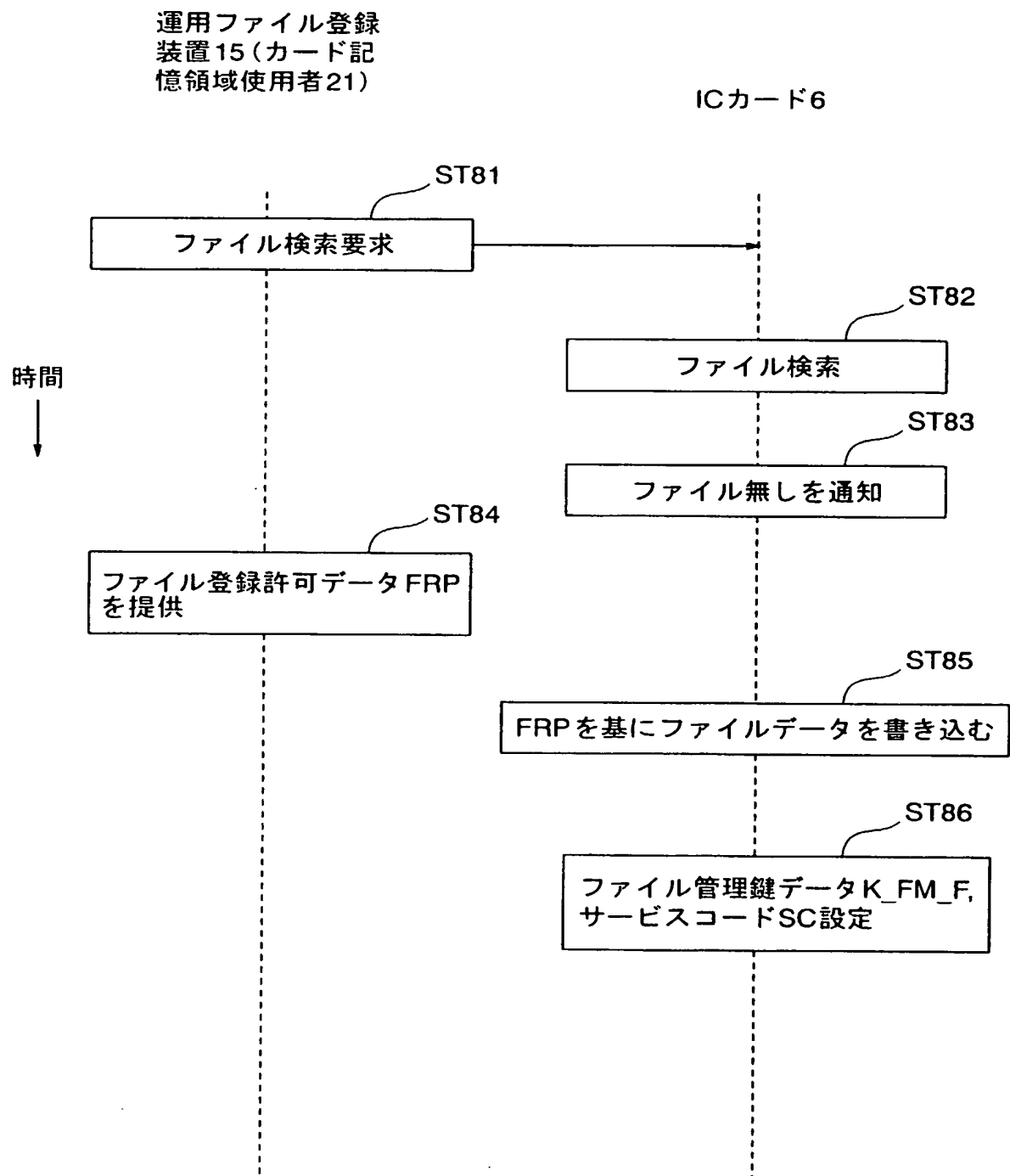
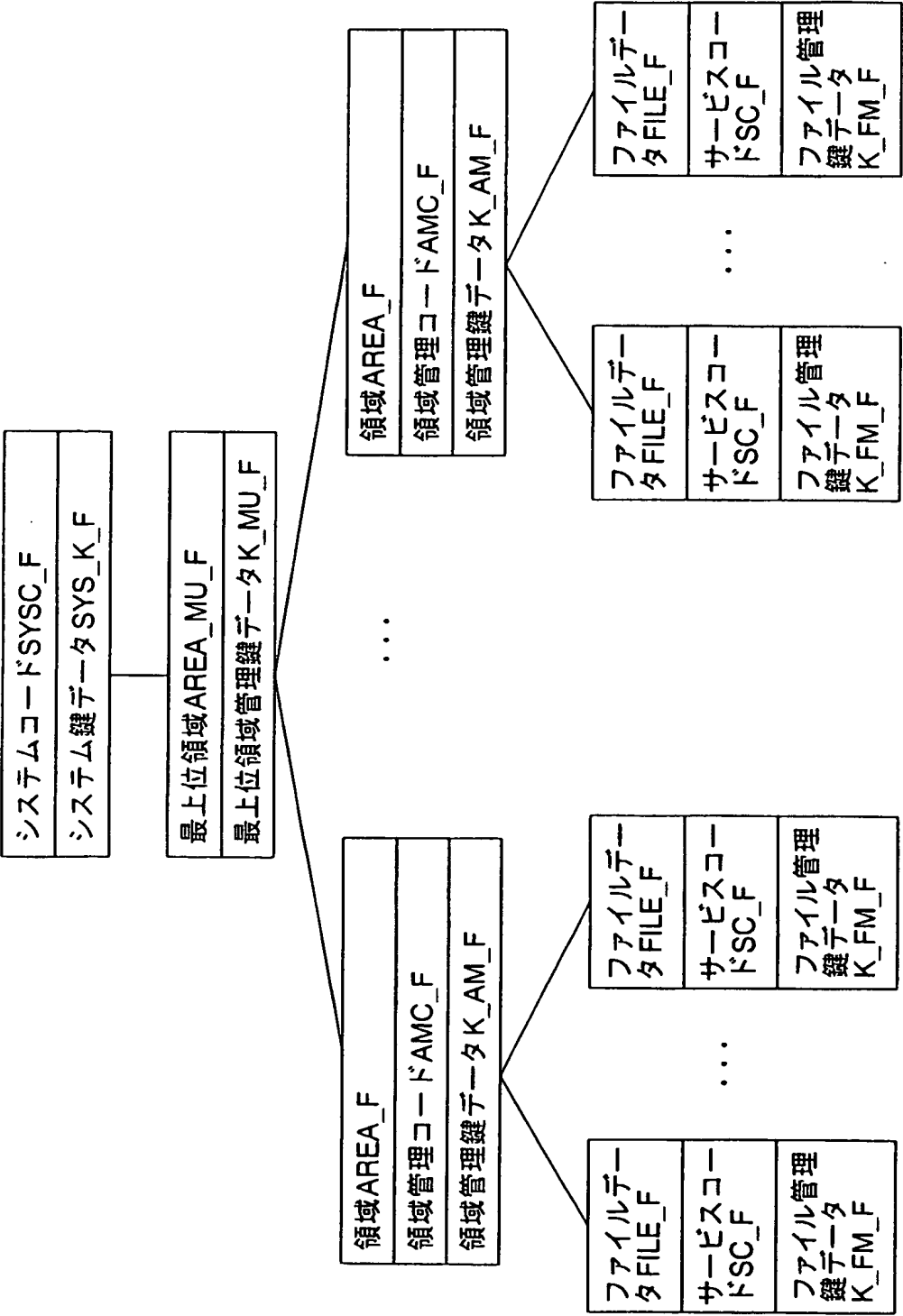


FIG. 25



最上位領域AREA\_MU\_F

FIG. 26

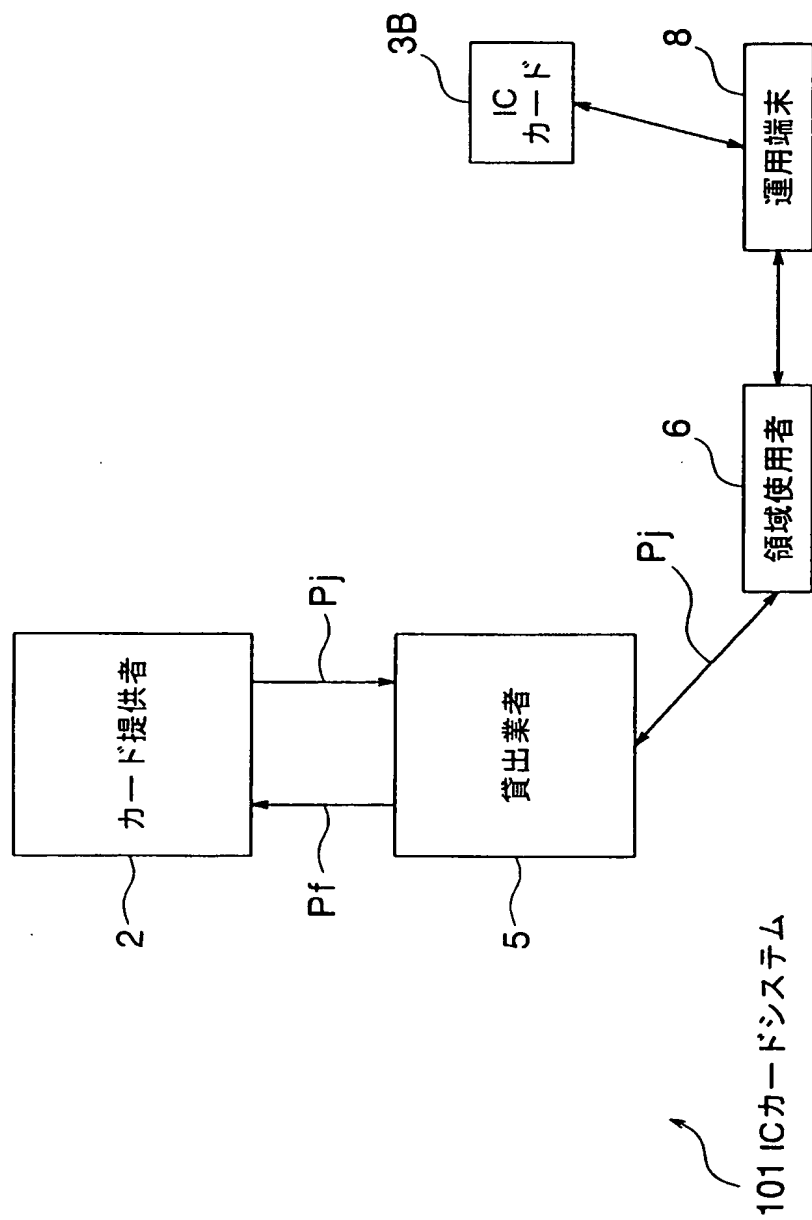


FIG. 27

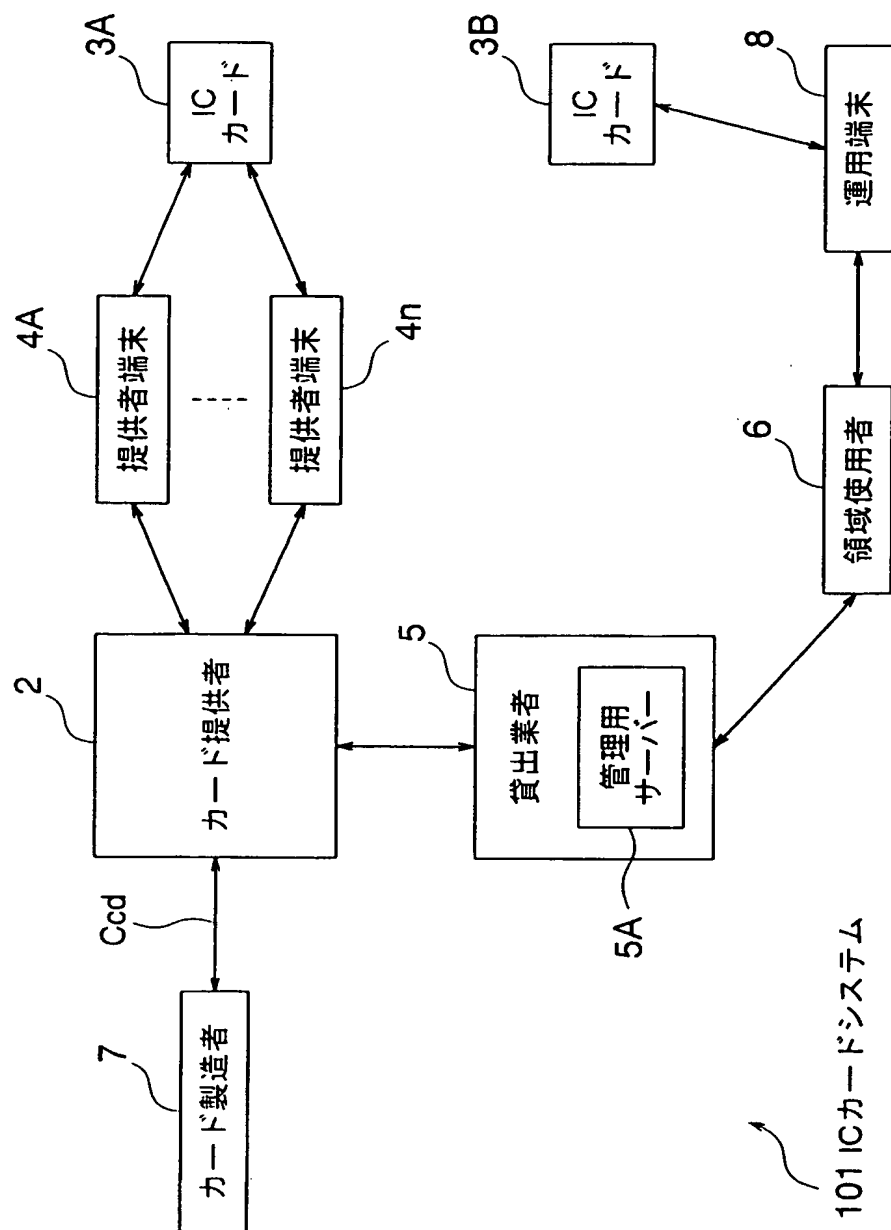




FIG. 28

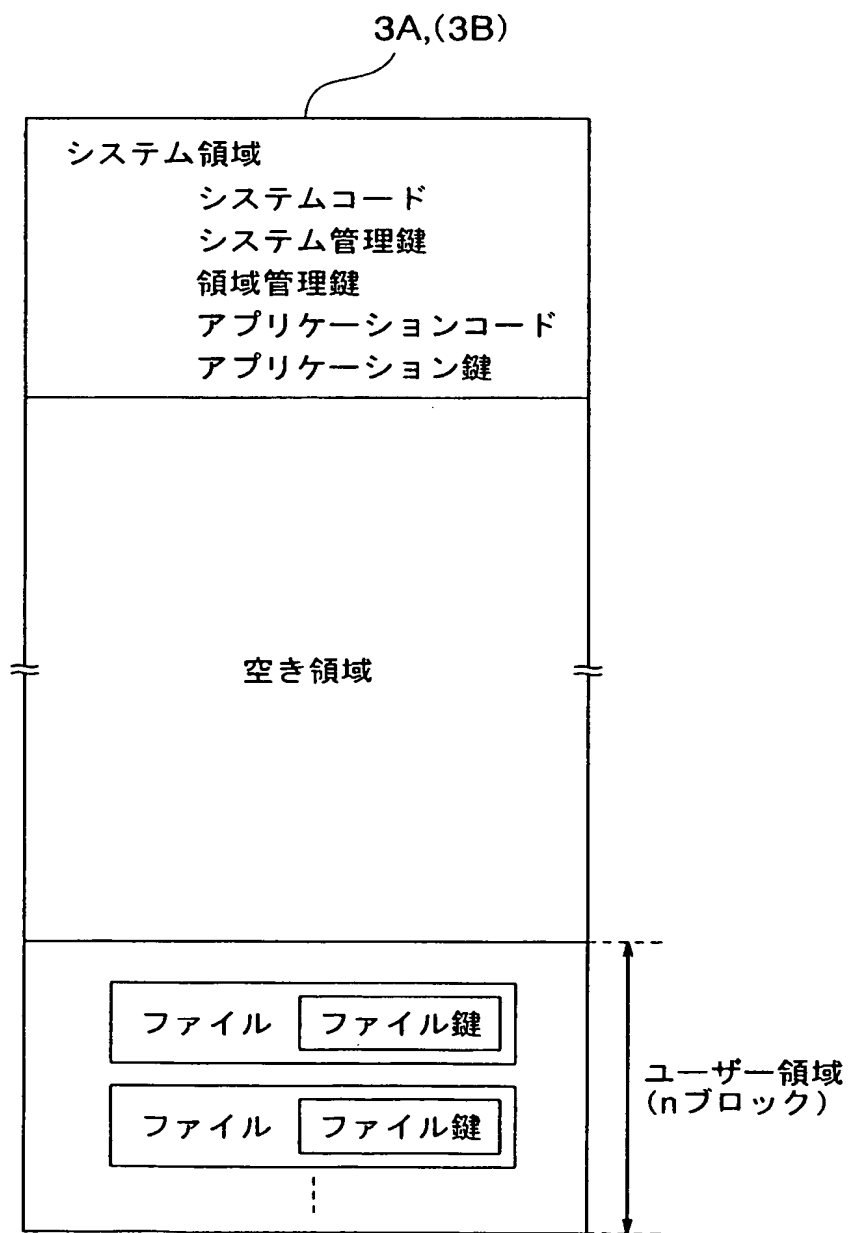


FIG. 29

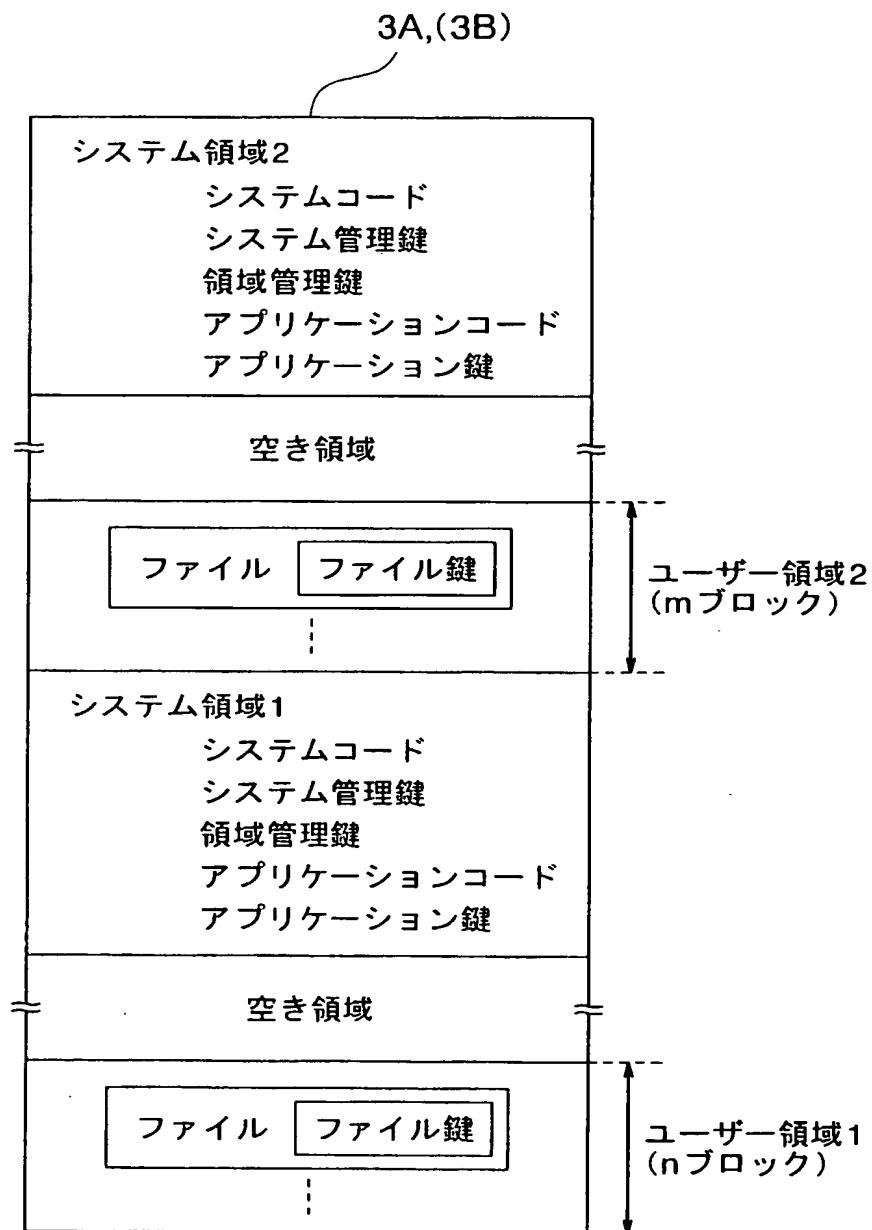


FIG. 30

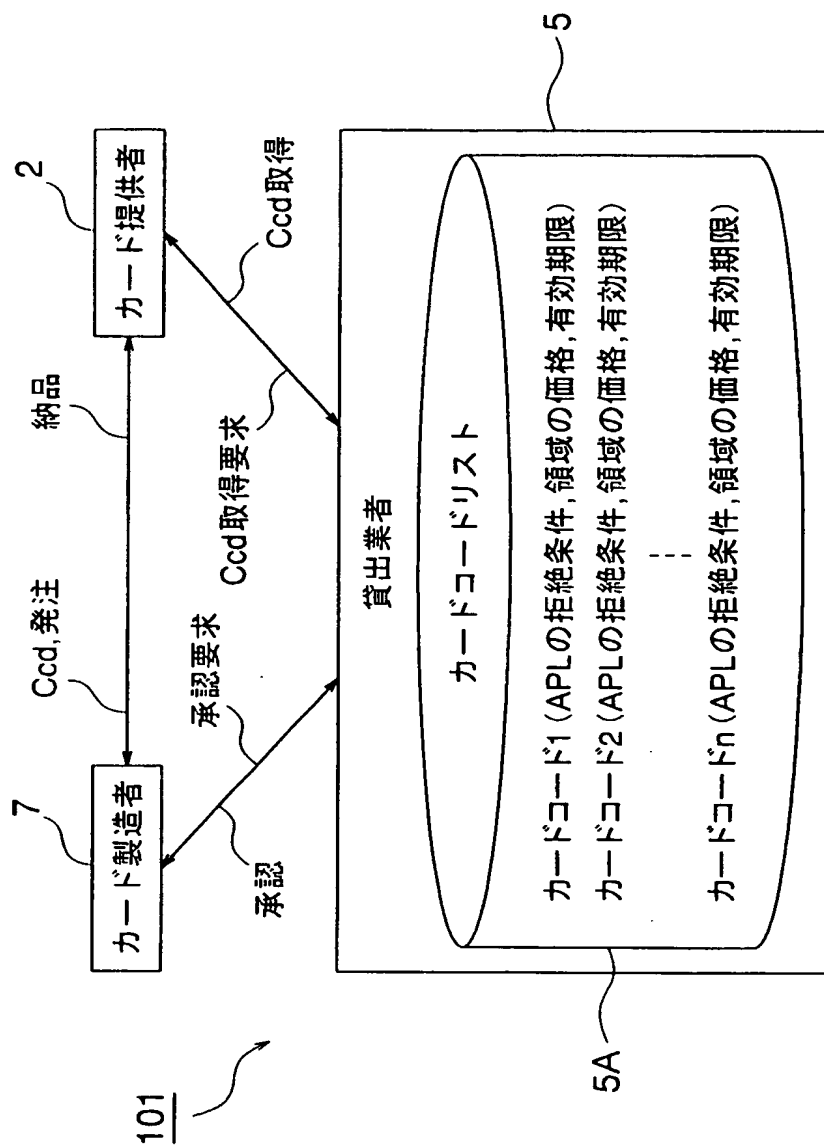


FIG. 31

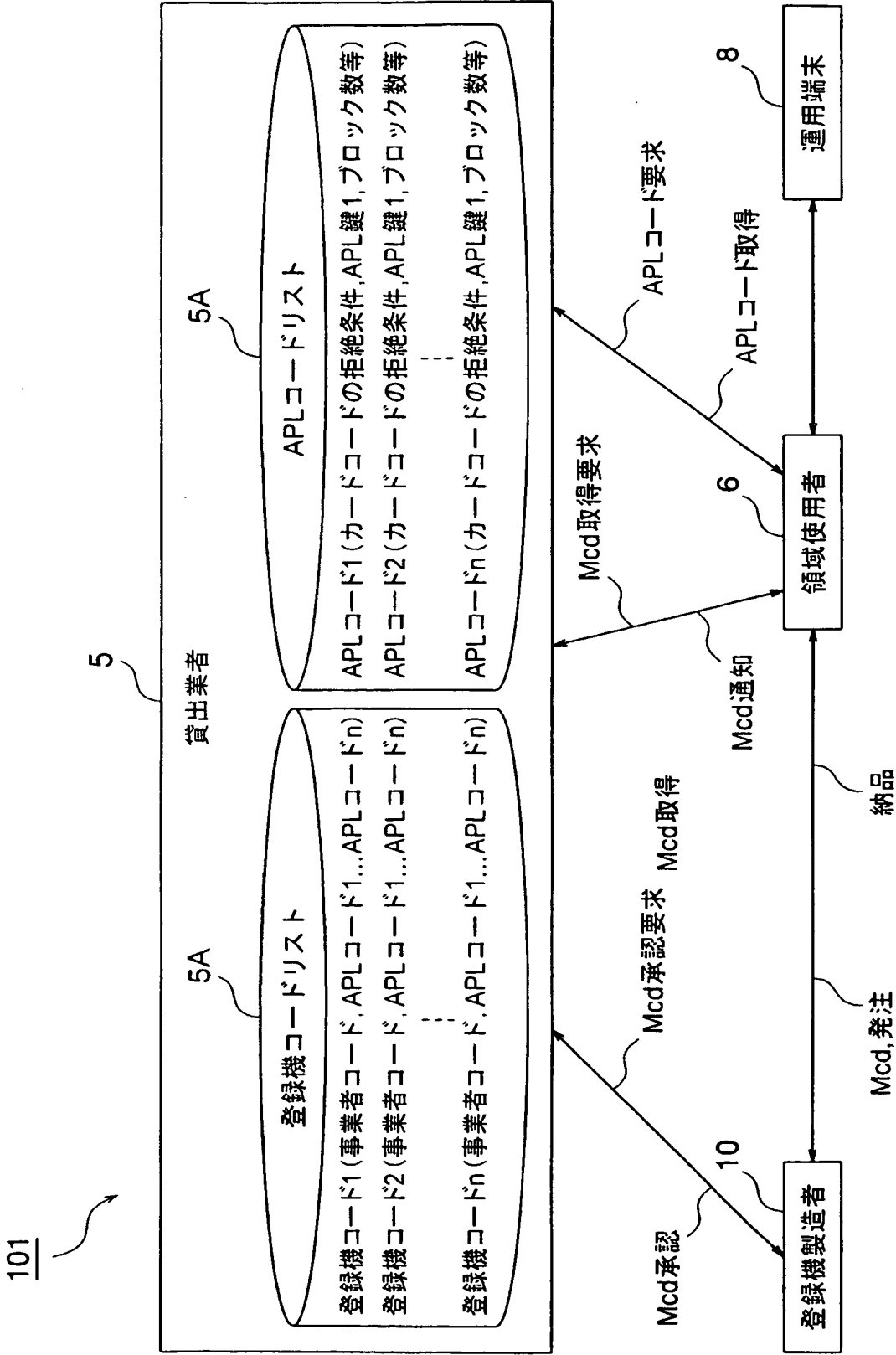


FIG. 32

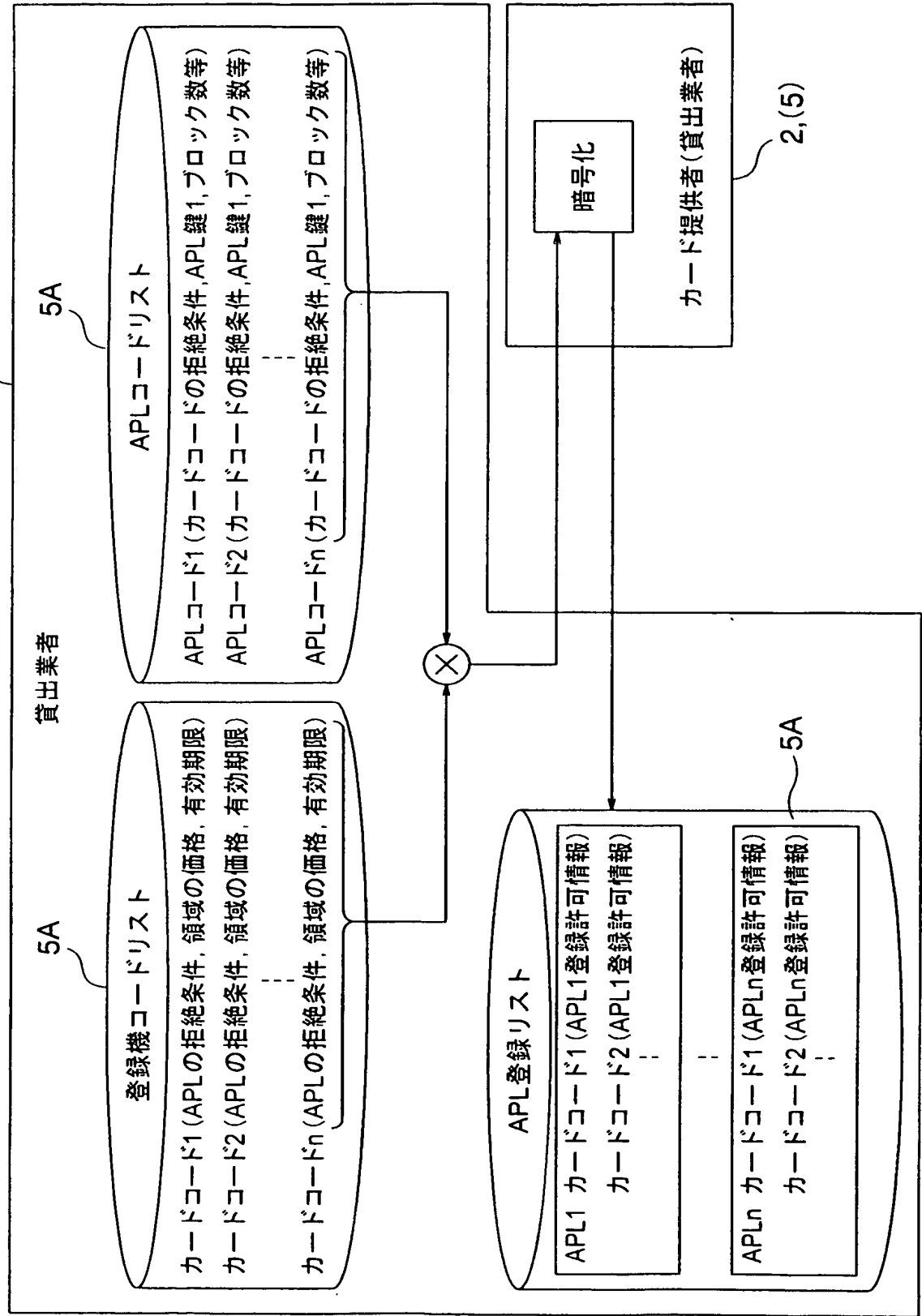
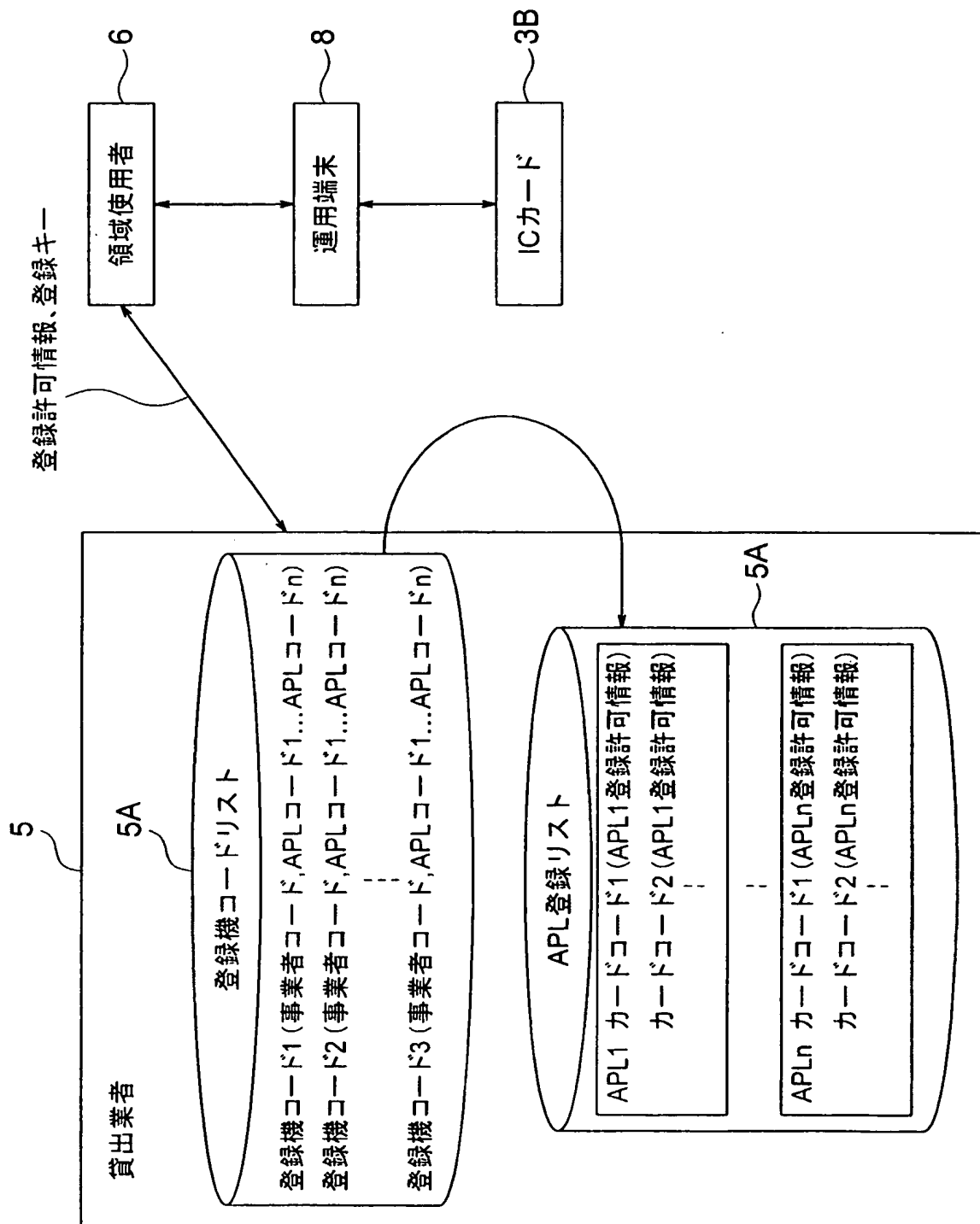


FIG. 33



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/02992

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F17/60, G06K17/00, G06K19/00, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F17/60, G06K17/00, G06K19/00, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2001

Kokai Jitsuyo Shinan Koho 1971-2001 Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-120300 A (Fujitsu Limited) 30 April, 1999 (30.04.99) Full text; all drawings & EP 908855 A2 & US 6003113 A1 & CN 1214488 A	1-30
A	JP 10-105472 A (Toshiba Corporation) 24 April, 1998 (24.04.98) Full text; all drawings & EP 798674 A2 & US 5929428 A1 & CN 1174355 A	1-30
A	JP 9-128505 A (TOPPAN PRINTING CO., LTD.) 16 May, 1997 (16.05.97) Full text; all drawings (Family: none)	1-30

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
18 July, 2001 (18.07.01)Date of mailing of the international search report  
31 July, 2001 (31.07.01)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F17/60, G06K17/00, G06K19/00, G09C1/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F17/60, G06K17/00, G06K19/00, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996

日本国公開実用新案公報 1971-2001

日本国実用新案登録公報 1996-2001

日本国登録実用新案公報 1994-2001

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 11-120300 A (富士通株式会社) 30.4月.1999 (30.04.99) 全文, 全図 & EP 908855 A2 & US 6003113 A1 & CN 1214488 A	1-30

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」同一パテントファミリー文献

国際調査を完了した日

18.07.01

国際調査報告の発送日

31.07.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

前田 仁

5N

2945

電話番号 03-3581-1101 内線 6915



## C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 10-105472 A (株式会社東芝) 24.4月.1998 (24.04.98) 全文, 全図 & EP 798674 A2 & US 5929428 A1 & CN 1174355 A	1-30
A	JP 9-128505 A (凸版印刷株式会社) 16.5月.1997 (16.05.97) 全文, 全図 (ファミリーなし)	1-30